Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All product, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Radiation Norm

This equipment has been tested and found to comply with limits for a Class B digital device pursuant to 47 CFR, Part 2 and Part 15 of the Federal Communication Commission (FCC) rules.

CE Radiation Norm

This equipment has been tested and found to comply with the limits of the European Council Directive 99/5/EC on the approximation of the law of the member states relating to EN 300 328 V1.4.1 (2003-04), EN 301 489-1 V1.4.1 (2002-08) and EN 301 489-17 V1.2.1 (2002-08).

FCC & CE Compliance Statement

These limits are designed to provide reasonable protection against radio interference in a residential environment. This equipment can generates, uses and radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment ON and OFF, the user is encouraged to try to reduce the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connect to
- Consult a dealer or an experienced technician for assistance

CAUTION!

The Federal Communication Commission warns the user that changes or modifications to the unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Contents

Chapter 1 Introduction

Congratulations on your purchase of this outstanding 4 Ports 11g Wireless ADSL2/2+ Router. This device is an IEEE 802.11g Wireless and 4 Port Switch built-in ADSL2/2+ Router that allows ADSL/ADSL2/ADSL2+ connectivity while providing Wireless LAN capabilities for residential, industries and SOHO environments. Wireless-G or the so-called 11g is the upcoming 54Mbps wireless networking standard that's almost 5 times faster than the widely deployed Wireless-B or the so-called 11b products found in homes, businesses, and public wireless hotspots around the world.

ADSL2/2+ is a transmission technology used to carry user data over a single twisted-pair line between the Central Office and the Customer Premises. The downstream data rates can go up to 24 Mbps and the upstream data rates can go up to 1Mbps with length reach up to 22Kft for ADSL2/2+ connection and 54Mbps transfer data rate for the 11g connection. This device allows ADSL2/2+ connectivity while providing Wireless LAN capabilities for home or office users. This asymmetric nature lends itself to applications such as Internet access and video delivery.

With minimum setup, you can install and use the router within minutes.

1.1 Features

- **ADSL Standards Compliance**
  - Full rate ANSI T1.413 Issue2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
  - ITU G.992.3, ITU G.992.5 and READSL2 ADSL2/2+ standards compliant.
  - Support ADSL2/2+ Annex L and Annex M features.
  - Downstream and Upstream data rates up to 24Mbps and 1Mbps.
  - Reach length up to 22Kft.
  - Support Dying Gasp functionality.

- **ATM and PPP Protocols**
  - Support ATM ALL0, ALL2 & ALL5.
  - Support OAM F4/F5 loop back.
  - Support up to 8PVCs.
  - Multiple Protocols over AAL5 (RFC 2684 / RFC 1483).
  - Support Bridged and Routed Ethernet Encapsulation.
  - Support VC and LLC based Multiplexing.
  - Support PPPoA (RFC 2364) standard.
  - Support PPPoE (RFC 2516) standard.
  - Support UBR, CBR, rt-VBR and nrt-VBR Traffic shaping QoS.
  - Support PPP Half-Bridge

- **Network Protocols & Features**
  - IP Routing – RIPv1 and RIPv2.
  - Support Static Routing.
  - Support DHCP Server, Relay and Client.
  - Support DNS Relay.
  - Support SNMP functionality.
  - Support IP QoS features.
  - Support IGMP functionality
  - Support IP Filter and MAC Filter functionality
  - URL Blocking features supported.
  - Support Port Forwarding features.
  - Support Port Triggering features.
  - Support DMZ functionality.
  - Support VPN Pass-Through.
  - Built-in Diagnostic Tools.
  - Built-in Firewall features.

- **Bridging**
  - Support IEEE 802.1d Transparent Bridging.
  - Support WAN Bridge functionality.
  - Support MAC Learning Address features.

- **IEEE 802.11g Wireless Standards**
  - IEEE 802.11b/g standards compliant.
  - Support data rates up to 54Mbps (Auto-Rate Capable).
  - Support OFDM (64QAM, 16QAM, QPSK, BPSK) and DSSS (DBPSK, DQPSK, CCK) modulation.
  - Conforms to Wireless Ethernet Compatibility Alliance (WECA) Wireless Fidelity (Wi-Fi) Standard.
  - Support WEP/WPA/WPA2/802.1X Encryption for data security.
  - Support AP Client features.
  - Support Wireless Access Control functionality.
  - Support WDS features.
  - Support 2.412GHZ ~ 2.484GHz frequency ranges.

- **Management**
  - Web-based Configuration / Management.
  - Support FTP/TFTP/Telnet Management / Configuration.
  - Support Remote Access Management / Configuration.
  - Firmware upgrade and Reset to default via Web management.
  - Restore factory default setting via Web or hardware reset button.
  - WAN and LAN connection statistics.
  - Support Password Authentication.
  - Device System Log.

- **Ethernet Standards**
  - Built-in 4 Ports 10/100Mbps Ethernet Switch which compliant with IEEE 802.3x standards
  - Automatic MDI/MDI-X crossover for 100BASE-TX and 10BASE-T ports.
  - Auto-negotiation and speed-auto-sensing support.
  - Port based VLAN supported in any combination.

1.2 Scope

This document provides the descriptions and usages for the 4 Ports 11g Wireless ADSL2/2+ Router's Web pages that are used in the configuration and setting process. Both basic and advanced descriptions and concepts are discussed. To help the reader understand more about these Web pages, some questions and answers (Q&A) are appended after the definition of each Web page along with the appendices at the end of the guide.

1.3 Audience

This document is prepared for use by those customers who purchase the 4 Ports 11g Wireless ADSL2/2+ Router and using the provided or embedded firmware. It assumes the reader has a basic knowledge of ADSL/ADSL2/ADSL2+, Wireless and networking.

1.4 Document Structure

Chapter 1: Introduction, provides a brief introduction to the product and user guide.

Chapter 2: Knowing The 4 Ports 11g Wireless ADSL2/2+ Router, provides device specifications and hardware connection mechanism.

Chapter 3: Setting Up TCP/IP In Windows, provides Windows system Network's configurations.

Chapter 4: Device Administration, describes the pages found under the Admin menu. These pages allow the user to view, change, edit, update, and save the 4 Ports 11g Wireless ADSL2/2+ Router's configurations or settings.

Appendix A: Router Terms, provides an introduction to basic Router Terms.

Appendix B: Frequently Asked Questions, is a compilation of useful questions regarding the 4 Ports 11g Wireless ADSL2/2+ Router.

Appendix C: Troubleshooting Guide, is a compilation of questions and answers relating to common problems dealing with Windows networking and the 4 Ports 11g Wireless ADSL2/2+ Router Configurations.

Appendix D: Glossary, provides definitions of terms and acronyms of this 4 Ports 11g Wireless ADSL2/2+ Router.

1.5 System Requirement

Check and confirm that your system confirm the following minimum requirements:

- Personal computer (PC/Notebook).
- Pentium III compatible processor and above.
- Ethernet LAN card or IEEE 802.11b or IEEE 802.11g Wireless adaptor installed with TCP/IP protocol.
- USB Port (Optional)
- 64 MB RAM or more.
- 50 MB of free disk space (Minimum).
- Internet Browser.
- CD-ROM Drive.

1.6 Packet Contents

The 4 Ports 11g Wireless ADSL2/2+ Router package contains the following items:

- One 4 Ports 11g Wireless ADSL2/2+ Router
- One Power Adapter
- One RJ-11 ADSL Cable
- One CAT-5 Ethernet Cable
- One CD-ROM (Driver / Manual / Quick Setup Guide)

If any of the above items are damaged or missing, please contact your dealer immediately.

Chapter 2 Knowing The 4 Ports 11g Wireless ADSL2/2+ Router

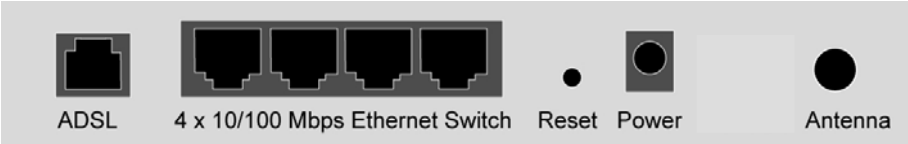
2.1 Front Panel:

The 4 Ports 11g Wireless ADSL2/2+ Router's LEDs indicators display information about the device's status.

PWR	Lights up when 4 Ports 11g Wireless ADSL2/2+ Router is powered on.
WL ACT	Lights up when Wireless system is ready.
	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is sending/receiving data.
1	Blinking when Port 1 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
2	Blinking when Port 2 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
3	Blinking when Port 3 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
4	Blinking when Port 4 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
ADSL	Lights up when a successful ADSL2/2+ connection is established.
	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is sending/receiving data.
PPP	Lights up when a PPP connection is established.

2.2 Back Panel:

The back panel of the 4 Ports 11g Wireless ADSL2/2+ Router contains ADSL, Ethernet Switches, Reset, Power Adapter connection and 2.4GHz Dipole Antenna connector.



ADSL	Port for connecting to the ADSL2/2+ Service Provider.
Ports 1~4	Four 10/100Mbps Ethernet Ports for connecting to the network devices
Power	Power adapter connector.
Antenna	2.4GHz Dipole Antenna.

All the Ethernet port of the 4 Ports 11g Wireless ADSL2/2+ Router supports auto-crossover capability.

RESET Button:
Reboot & Restore the 4 Ports 11g Wireless ADSL2/2+ Router to factory defaults.

Resetting Factory Defaults:

The reboot and restore to factory defaults feature will set the device to its factory default configuration by resetting the 4 Ports 11g Wireless ADSL2/2+ Router.

To Reset the 4 Ports 11g Wireless ADSL2/2+ Router:

- Ensure that the device is powered on.
- Press the Reset button for 10~15 seconds and release. The LED indicators will turns OFF and ON again indicates that the reset is in progress. Do not power off the device during the reset process.
- Reset is completed when the LED indicator return to steady green. The default settings are now restored.

2.3 Connection Mechanism:

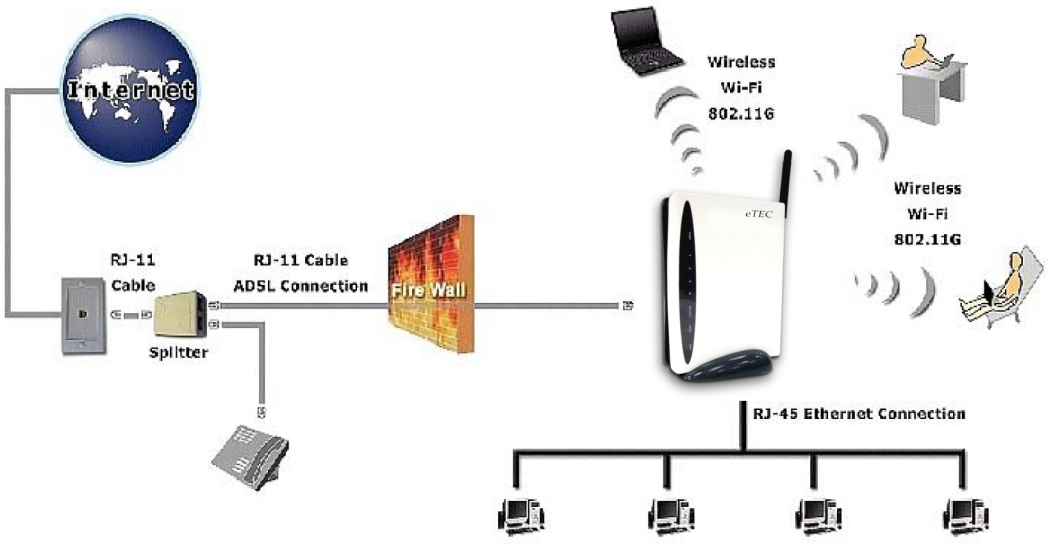
This section describes the hardware connection mechanism of 4 Ports 11g Wireless ADSL2/2+ Router on your Local Area Network (LAN) connected to the Internet, how to configure your 4 Ports 11g Wireless ADSL2/2+ Router for Internet access or how to manually configure your Internet connection.

You need to prepare the following items before you can establish an Internet connection through your 4 Ports 11g Wireless ADSL2/2+ Router:

1. A computer/notebook which must have an installed Ethernet Adaptor and an Ethernet Cable, or
2. A computer/notebook which have Wireless-b or Wireless-g wireless adaptor properly installed.
3. ADSL/ADSL2/ADSL2+ service account and configuration information provided by your Internet Service Provider (ISP). You will need one or more of the following configuration parameters to connect your 4 Ports 11g Wireless ADSL2/2+ Router to the Internet:

    a. VPI/VCI parameters
    b. Multiplexing Method or Protocol Type or Encapsulation Type
    c. Host and Domain Names
    d. ISP Login Name and Password
    e. ISP Domain Name Server (DNS) Address
    f. Fixed or Static IP Address.

Figure below shows the overall hardware connection mechanism of your 4 Ports 11g Wireless ADSL2/2+ Router.



Following are the steps to properly connect your 4 Ports 11g Wireless ADSL2/2+ Router:

1. Turn off your computer/notebook.
2. Connect the ADSL port of your 4 Ports 11g Wireless ADSL2/2+ Router to the wall jack of the ADSL/ADSL2/ADSL2+ Line with a RJ-11 cable.
3. Connect the Ethernet cable (RJ-45) from your 4 Ports 11g Wireless ADSL2/2+ Router (Switch) to the Ethernet Adaptor in your computer.
4. Connect the Power adaptor to the 4 Ports 11g Wireless ADSL2/2+ Router and plug it into a Power outlet.

The Power light will lit after turning on the 4 Ports 11g Wireless ADSL2/2+ Router.
Auto and self-diagnostic process will turn the LED indicators ON and OFF during the process.

Use the Power Adaptor exclusively in combination with the equipment supplied and do not use any other kind of power adaptor for the equipment.

5. Turn on your computer.
6. Refer to the next section to setup or configure your system's Network Adaptor.

Chapter 3 Setting up the TCP/IP in Windows

The instruction in this chapter will help you configure your computers to be able to communicate with this 4 Ports 11g Wireless ADSL2/2+ Router.

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer/notebook on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

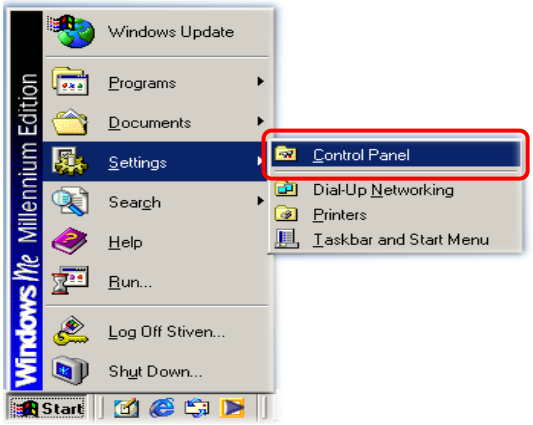
The following description assumes 4 Ports 11g Wireless ADSL2/2+ Router been set to factory default. (If not, please hold the reset button down for 5~10 seconds). The default of the 4 Ports 11g Wireless ADSL2/2+ Router's LAN IP is **192.168.1.1**.

Follow the procedures below to set your computer/notebook function as a **DHCP Client**.

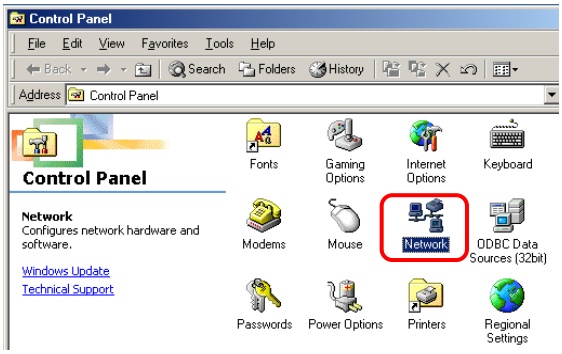
Restart and Reboot your Windows system might be necessary after setting your computer function as a DHCP Client. In order to properly activate your choice, click "OK" to restart your Windows system.

3.1 Windows ME / 98

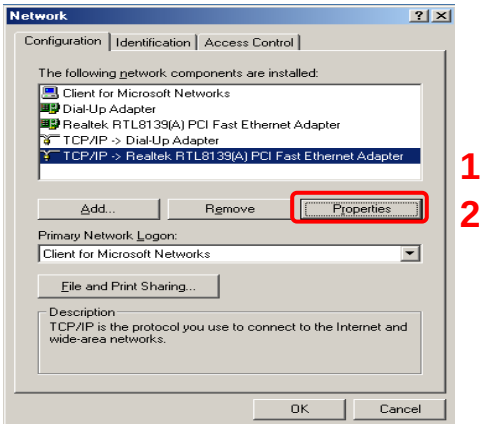
Step 1: Click **Start→Settings→Control Panel**.



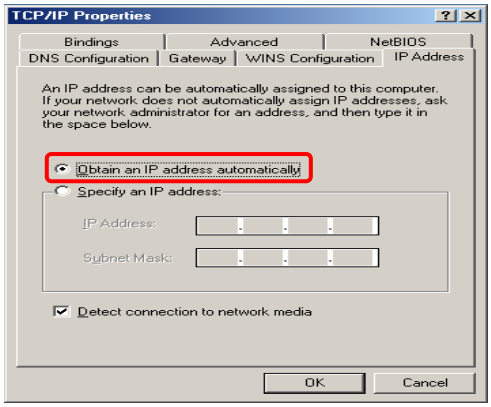
Step 2: Double-click the **Network** icon.



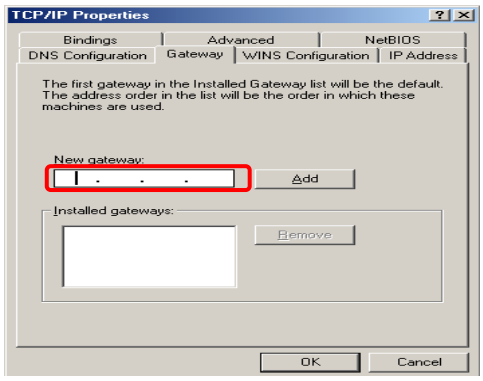
Step 3: Go to Configuration icon, select network adapter installed and click **Properties**.



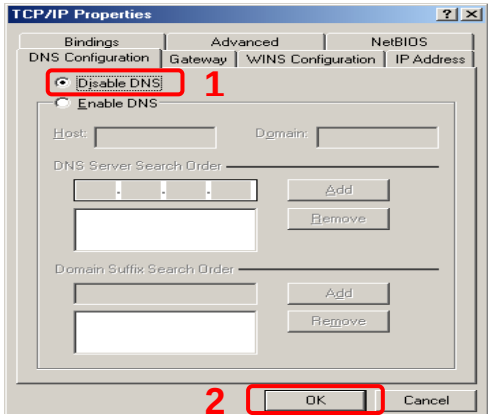
Step 4: Go to IP Address icon and select **Obtain an IP address**.



Step 5: Go to Gateway icon and erase all previous setting.

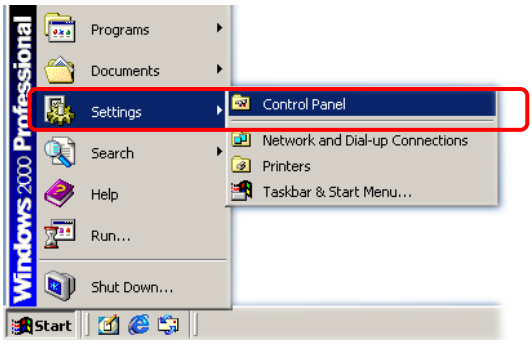


Step 6: Go to DNS Configuration icon, select **Disable DNS** and click **OK**.

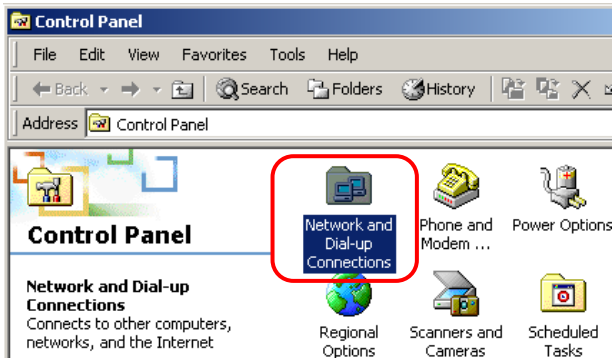


3.2 Windows 2000

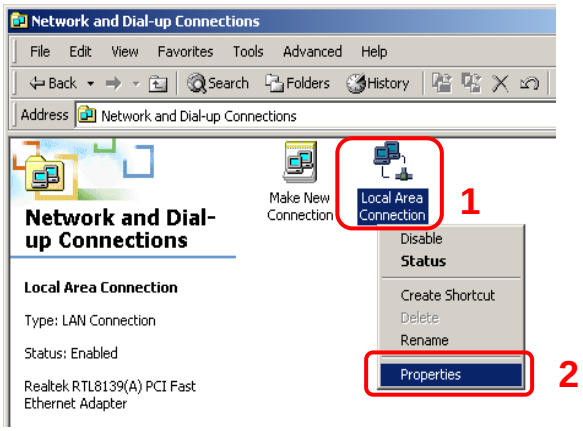
Step 1: Click **Start→Settings→Control Panel**.



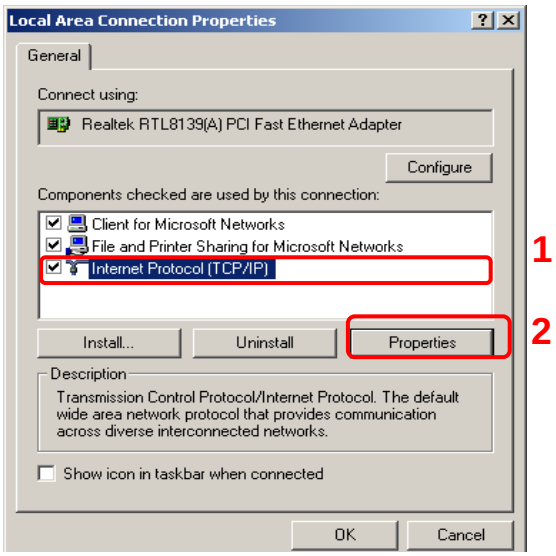
Step 2: Double-click the **Network and Dial-up Connections**.



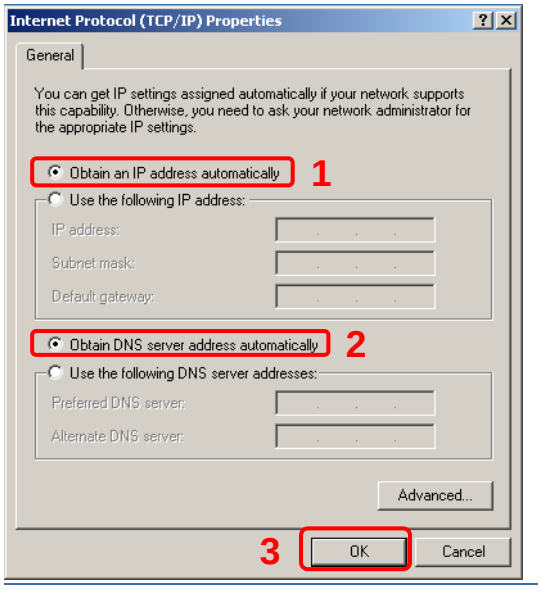
Step 3: Right Click the **Local Area Connection** and select **Properties**.



Step 4: Select **Internet Protocol (TCP/IP)** and click **Properties**.

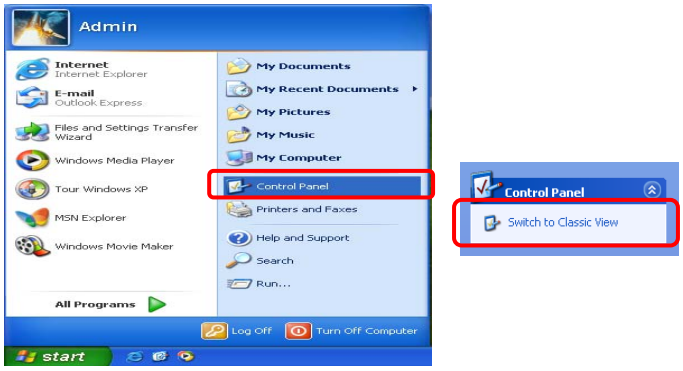


Step 5: Select **Obtain an IP address automatically** and **DNS server address automatically.** Then, click **OK**.

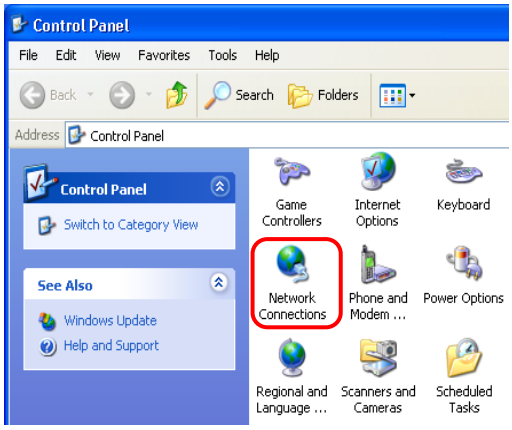


3.3 Windows XP

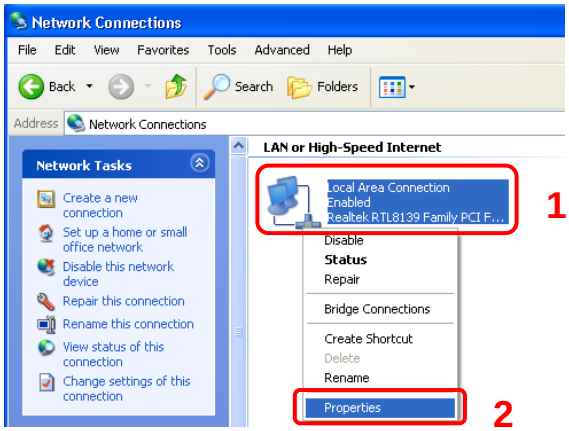
Step 1: Click **Start→Control Panel→Classic View**.



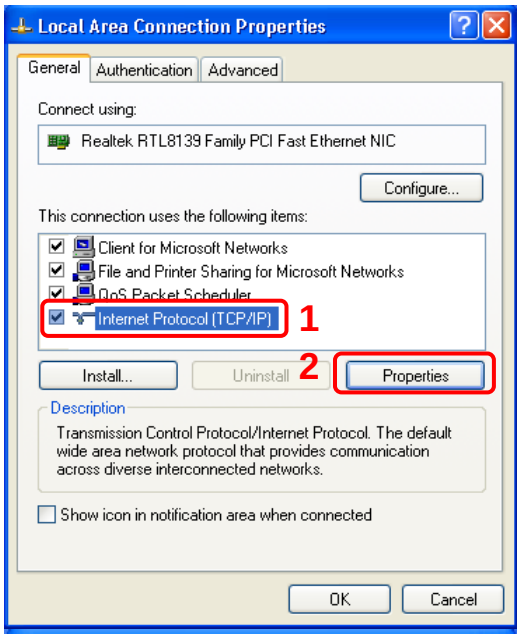
Step 2: Double-click the **Network Connections**.



Step 3: Right Click on the **Local Area Connection** and select **Properties**.

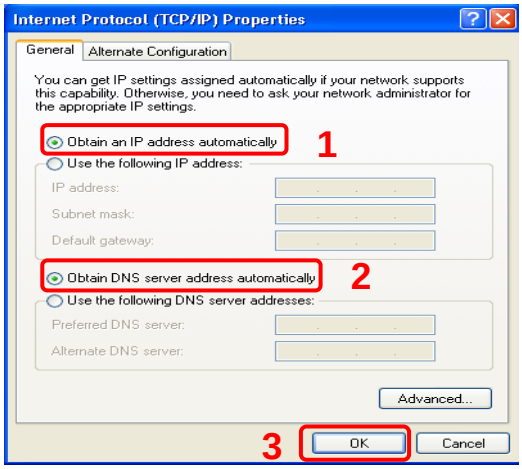


Step 4: Go to General icon, select **Internet Protocol (TCP/IP)** and click **Properties**.



Step 5: Go to General icon, select **Obtain an IP address automatically** and **DNS server address automatically**.

Then, click OK**.**

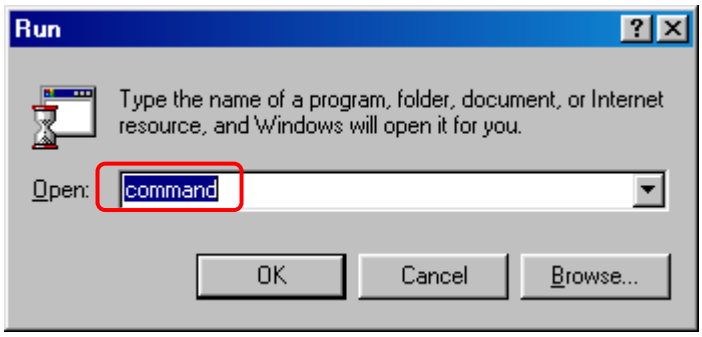


3.4 Checking TCP/IP Configuration

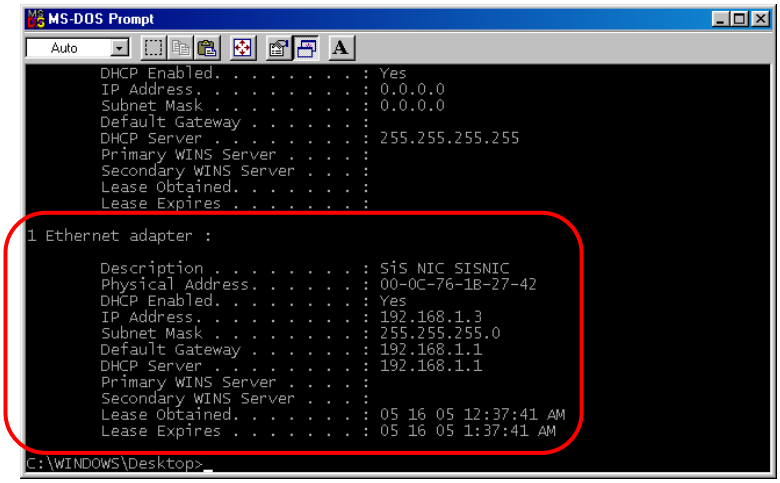
After your PC is configured and the system has rebooted, you can check the TCP/IP configuration using the following utility provided by your Windows system:

A. Windows 98/ME:

1. Click on **"Start"** and **"Run"**.
2. In the open field, enter **"Command",** then press **"OK"**.



3. In the command prompt, type **"Winipcfg"**, and then press **"Enter"**. All the Ethernet adapter information will be shown in the appears Windows. Check if you can get the following setting:

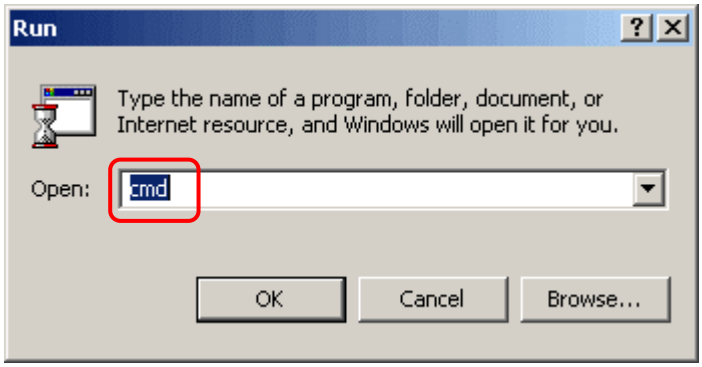


- The **IP Address** as **192.168.1.x**
- The **Subnet Mask** as **255.255.255.0**
- The **Default Gateway** as **192.168.1.1**

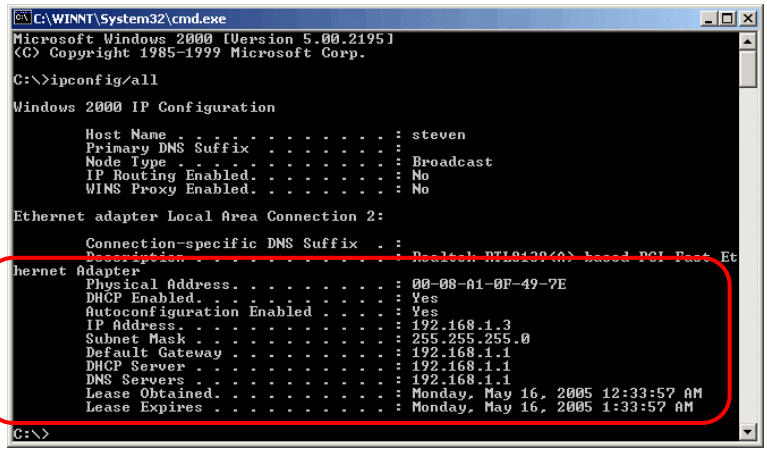
4. Type **"Exit"** to end up the MS-DOS Prompt.

B. Windows 2000:

1. Click **"Start"** and **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.



3. In the command prompt, type **"ipconfig /all"**, then press **"Enter"**.



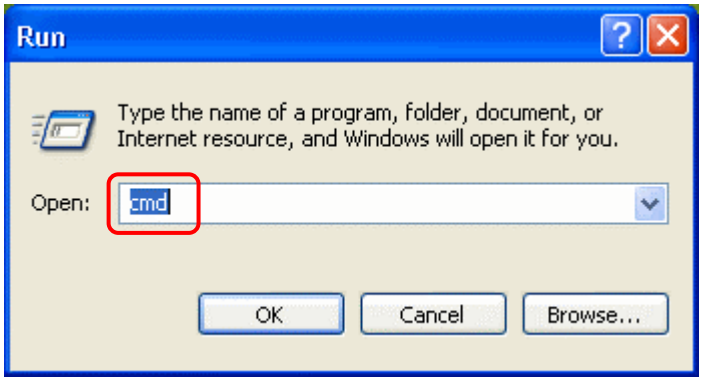
All the Ethernet adapter information will be shown in the appear Windows. Check if you can get the following setting:

- The **IP Address** as **192.168.1.x**
- The **Subnet Mask** as **255.255.255.0**
- The **Default Gateway** as **192.168.1.1**

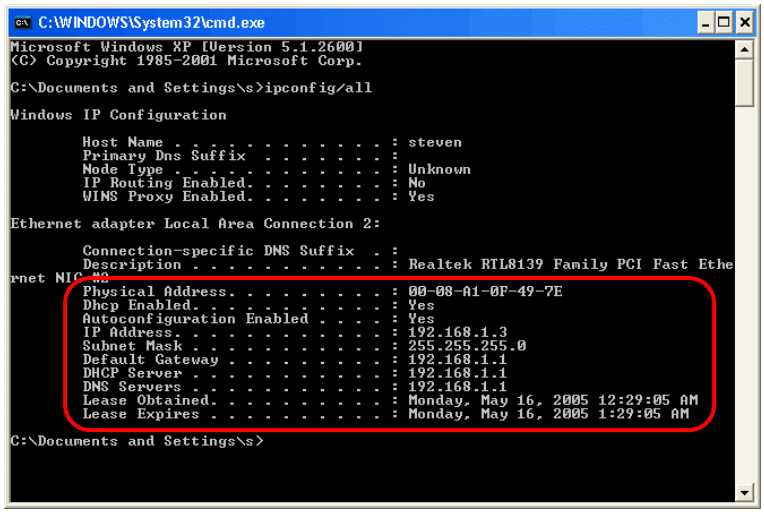
4. Type **"Exit"** to end up the process.

C. Windows XP:

1. Click **"Start"** and **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.



3. In the command prompt, type **"ipconfig /all"**, then press **"Enter"**



All the Ethernet adapter information will be shown in the appear Windows. Check if you can get the following setting:

- IP address as **192.168.1.x**
- The Subnet Mask as **255.255.255.0**
- the default gateway as **192.168.1.1**

4. Type **"Exit"** to end up the process.

Chapter 4 Device Administration

For your convenience, an Administrative Utility has been programmed into 4 Ports 11g Wireless ADSL2/2+ Router. This chapter will explain all the functions in this utility. All the 4 Ports 11g Wireless ADSL2/2+ Router based administrative tasks are performed through this web utility.

4.1 Login

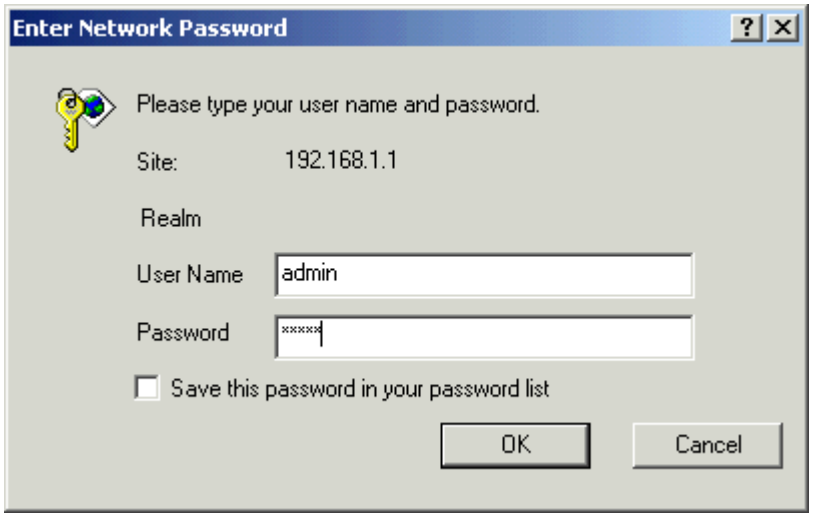
To access the 4 Ports 11g Wireless ADSL2/2+ Router Configuration screens, follow the following steps will enable you to log into the 4 Ports 11g Wireless ADSL2/2+ Router:

1. Launch the Web browser (Internet Explorer, Netscape, etc).

2. Enter the 4 Ports 11g Wireless ADSL2/2+ Router default IP address (Default Gateway) http://192.168.1.1 in the address bar then press Enter to Log in.

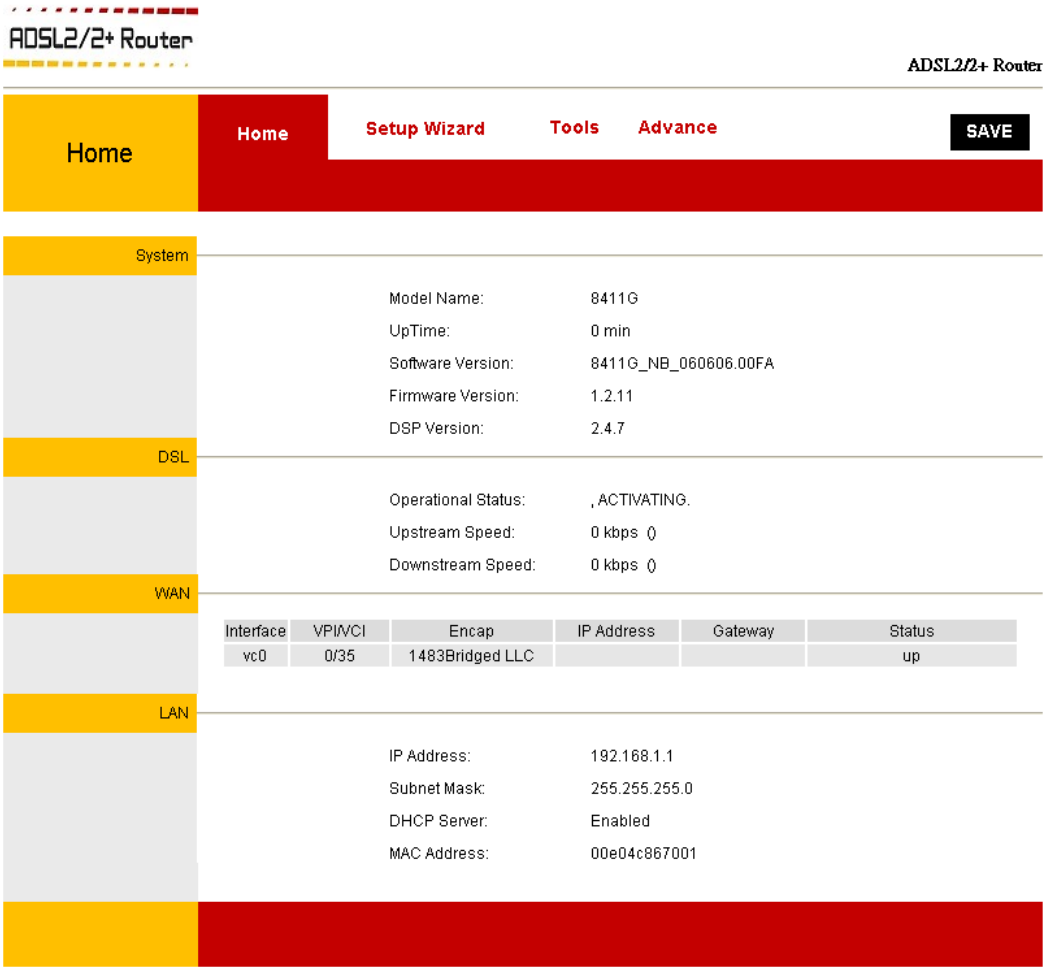
3. Entry of the username and password will be prompted. Enter the default login **"Username"** and **"Password"**: The default login Username of the administrator is **"admin"**, and the default login Password is **"admin"**.

Note that the Username and Password are case sensitive.



"Username" and **"Password"** can be changed after login. Refer to the **Tools** configuration section for further instruction.

Upon entering the address into the web browser, the system **HOME** page with all the device information will pop up as shown below:



- **Home:** The **Home** section show the current 4 Ports 11g Wireless ADSL2/2+ Router's connection status and System information.

- **Setup Wizard:** The **Setup Wizard** is a presetting wizard which meant to help you install the 4 Ports 11g Wireless ADSL2/2+ Router quickly and easily.

- **Tools:** The **Tools** section lets you carry out system commands, firmware update, device management and perform simple system tests.

- **Advanced:** The **Advanced** section lets you configure advanced features like Wireless, RIP, SNMP, IP QoS, Firewall, Access control, … etc.

- **System:** Shows the current device System Information.
  - ☑ **Model Name:** Shows the device Model Name.
  - ☑ **Uptime:** Shows the Ethernet connection time.
  - ☑ **Software Version:** Shows the device Software Version.
  - ☑ **Firmware Version:** Shows the device's Firmware Version.
  - ☑ **DSP Version:** Shows the device DSP code version.

- **DSL:** Shows the ADSL WAN connection status.
  - ☑ **Operational Status:** Shows the ADSL WAN connection status.
  - ☑ **Upstream Speed:** Shows the ADSL Upstream connection speed in Kbps.
  - ☑ **Downstream Speed:** Shows the ADSL Downstream connection speed in Kbps.

- **WAN:** Shows the WAN setting information and connection status.
  - ☑ **Interface:** The ISP selected for your ADSL connection..
  - ☑ **VPI/VCI:** Virtual Path Identifier (**VPI**) is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing. Virtual Channel Identifier (**VCI**) is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
  - ☑ **Encap:** The Encapsulation Type connected to the Internet (e.g. PPPoA, PPPoE, 1483 Routed, .. etc).
  - ☑ **IP Address:** The ADSL connection IP Address (Assigned by your ADSL ISP).
  - ☑ **Gateway:** The Gateway Address (Assigned by your ADSL ISP).
  - ☑ **Status:** The ADSL connection status.

- **LAN:** Shows the LAN setting information and connection status.
  - ☑ **Description:** This field displays the ADSL ISP name.
  - ☑ **Type:** Shows the connection type use by your ISP.
  - ☑ **IP:** This field displays the WAN IP address which will be provided by your ISP.
  - ☑ **State:** Shows the ADSL connection status.
  - ☑ **Online:** This field display your ADSL online time.
  - ☑ **Disconnect Reason:** Display the ADSL disconnect reason.

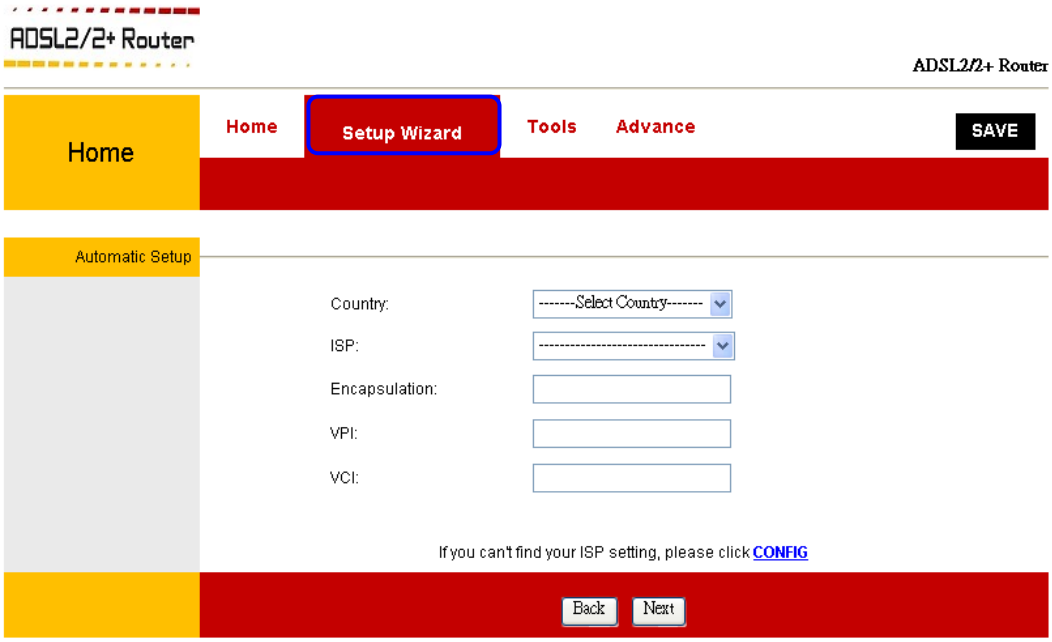
- **System Information:** Shows the current device connection status.

  - ☑ **IP Address:** The device's IP Address.
  - ☑ **Subnet Mask:** The device's Subnet Mask.
  - ☑ **DHCP Server:** The device's DHCP Server status.
  - ☑ **MAC Address:** MAC address of the PC.

4.2 Setup Wizard

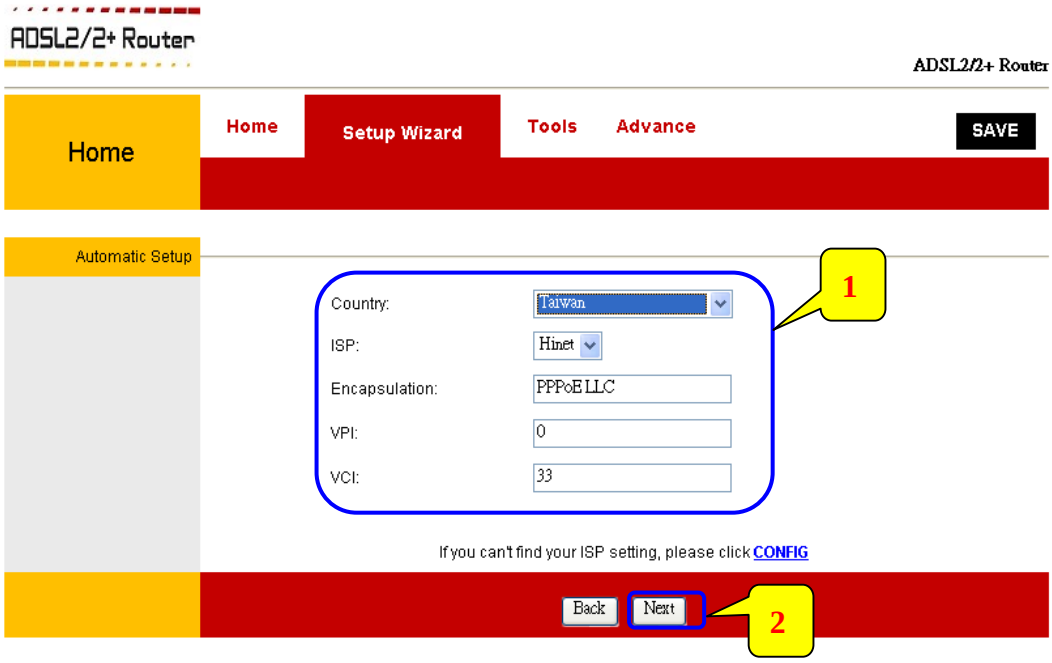
The **Setup Wizard** is a presetting wizard which meant to help you install the 4 Ports 11g Wireless ADSL2/2+ Router quickly and easily.

Click on **"Setup Wizard"** and the following screen will pop-up:



Follow the **"Steps"** describe below to complete your installation.

Step 1: Select your country from the **Country** list and the ADSL service provider from the **ISP** List (If there are more than two ISP in your country) and note the **"Encapsulation"** type and **"VPI & VCI"** setting. Click **"Next"** to continue.

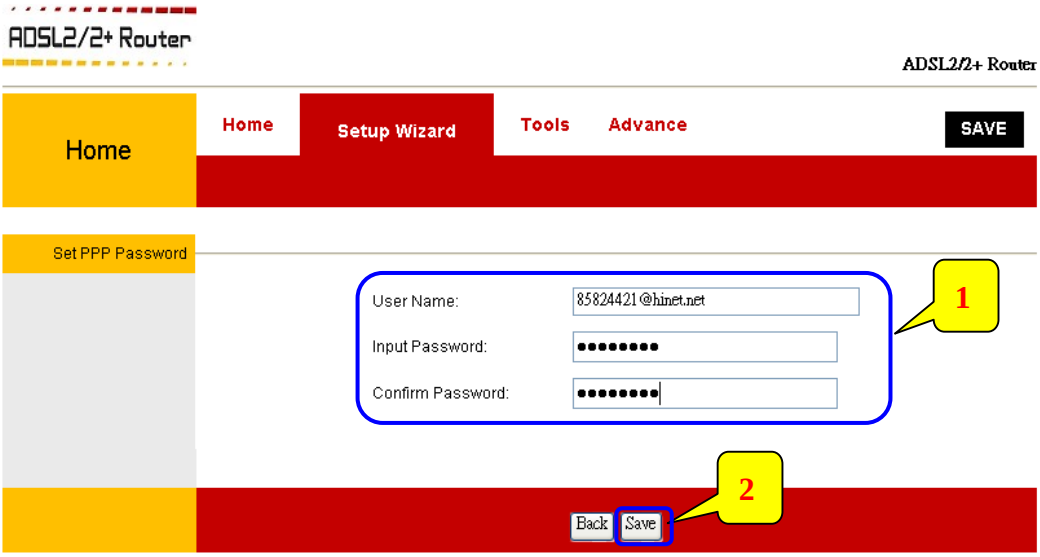


Click "ONFIG" if you can't find any available parameters from the presetting country list.

Check your ISP immediately for the setting/configuration details.

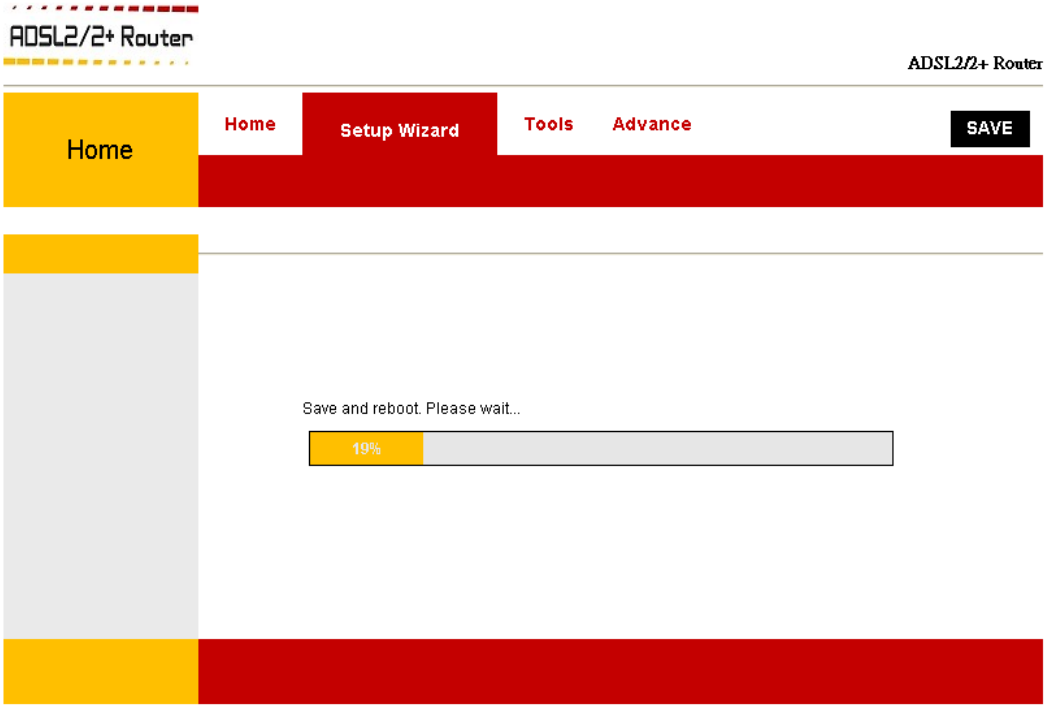
A. For countries with the following **"Encapsulation"** type after clicking the **"Next"** button at **Step 1**, you will enter into set PPP Username and Password window as shown below:

- ☑ **PPPoA VC-Mux**
- ☑ **PPPoA LLC**
- ☑ **PPPoE VC-Mux**
- ☑ **PPPoE LLC**

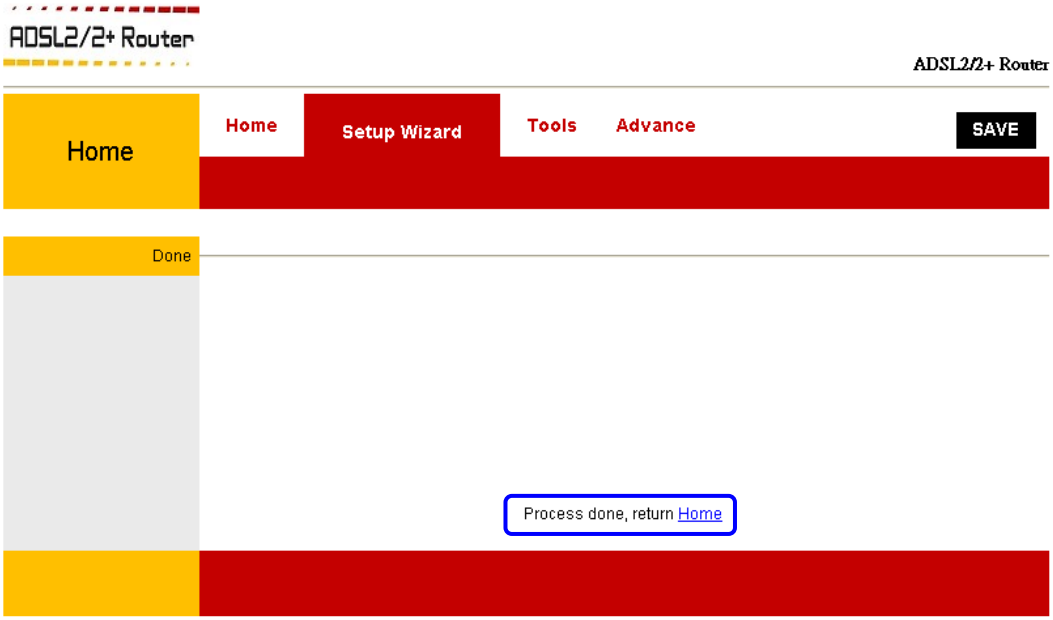


Manually enter your **"Username"** and **"Password"** which will be provided by your Service Provider (ISP).

Click **"Save"** after setup. The following window display indicates the save setting process.



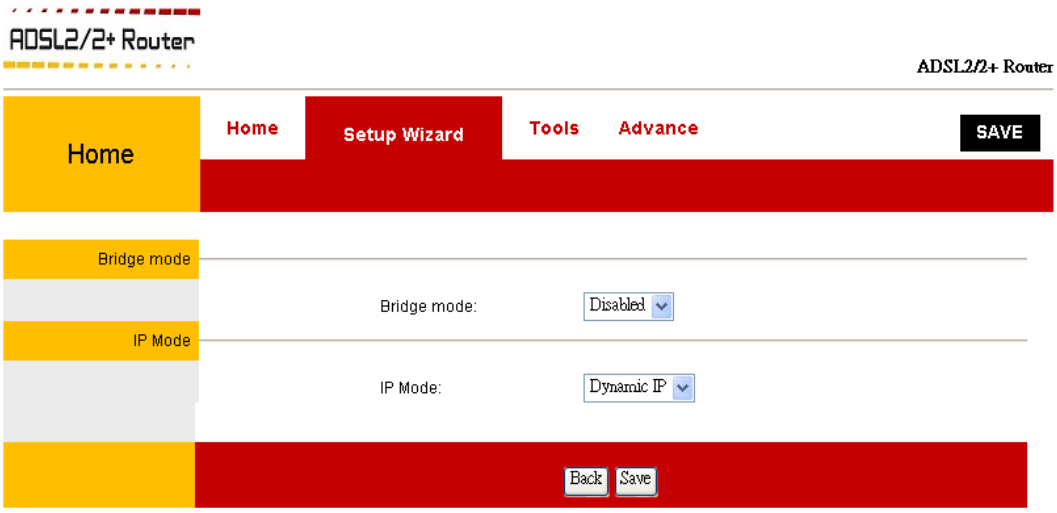
A **“Process Done”** screen will pop-up after the save setting process.



Click **“Home”** to return to the system Home page.

B. For countries with the following **"Encapsulation"** after clicking the **"Next"** button at **Step 1**, the following window will pop-up:

- ☑ **1483 Routed IP VC-Mux**
- ☑ **1483 Routed IP LLC**
- ☑ **1483 Bridged IP VC-Mux**
- ☑ **1483 Bridged IP LLC**



In this current window, you will find the following **Connection Type**:

1. Bridge Mode – Disabled (Default):

- When **Bridge Mode** is set to **"Disabled"**, please select **Dynamic IP** or **Static IP** from the IP Mode drop down manual.

  - ☑ **Dynamic IP:** When Dynamic IP mode is selected, nothing to be filled under this mode. Just click the **"Save"** button to confirm your setting.

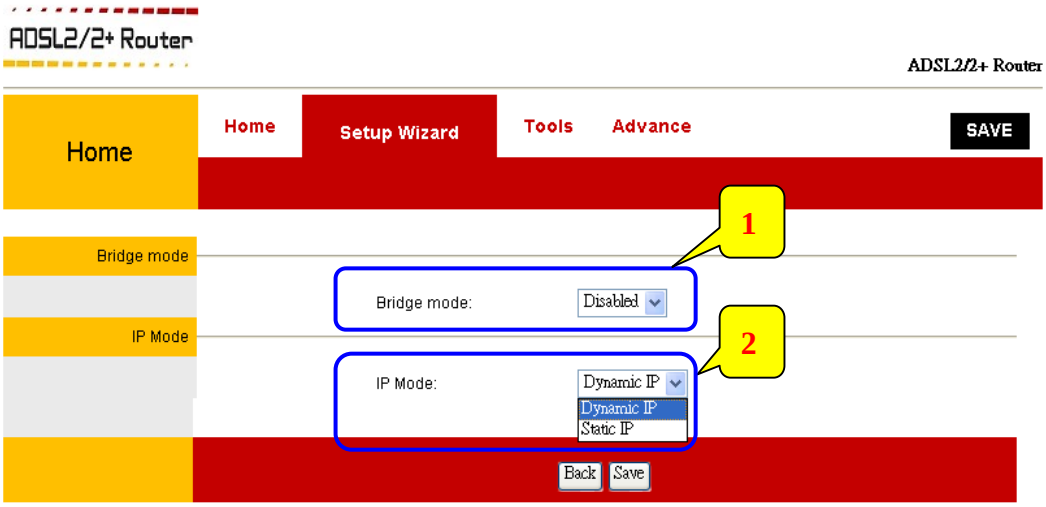
  - ☑ **Static IP:** When **Static IP** mode is selected, manually enter the **"Static IP Address"**, **"Subnet Mask"**, **"Gateway"** and **"DNS"** which will be provided by your ISP.

2. Bridge Mode – Enabled:

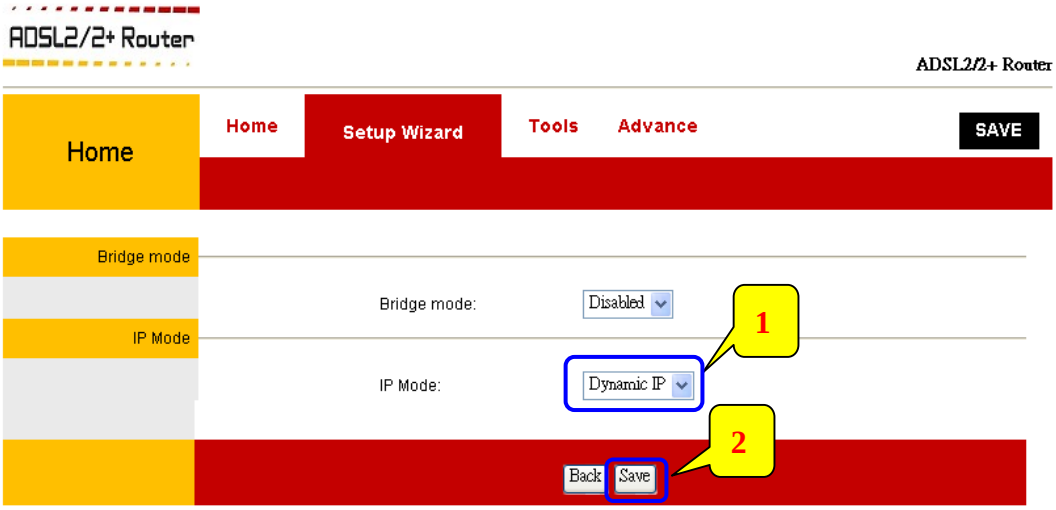
- Nothing to be filled under this mode. Just click the **"Save"** button to confirm your setting.

- **Bridge Mode – Disabled (Default):**

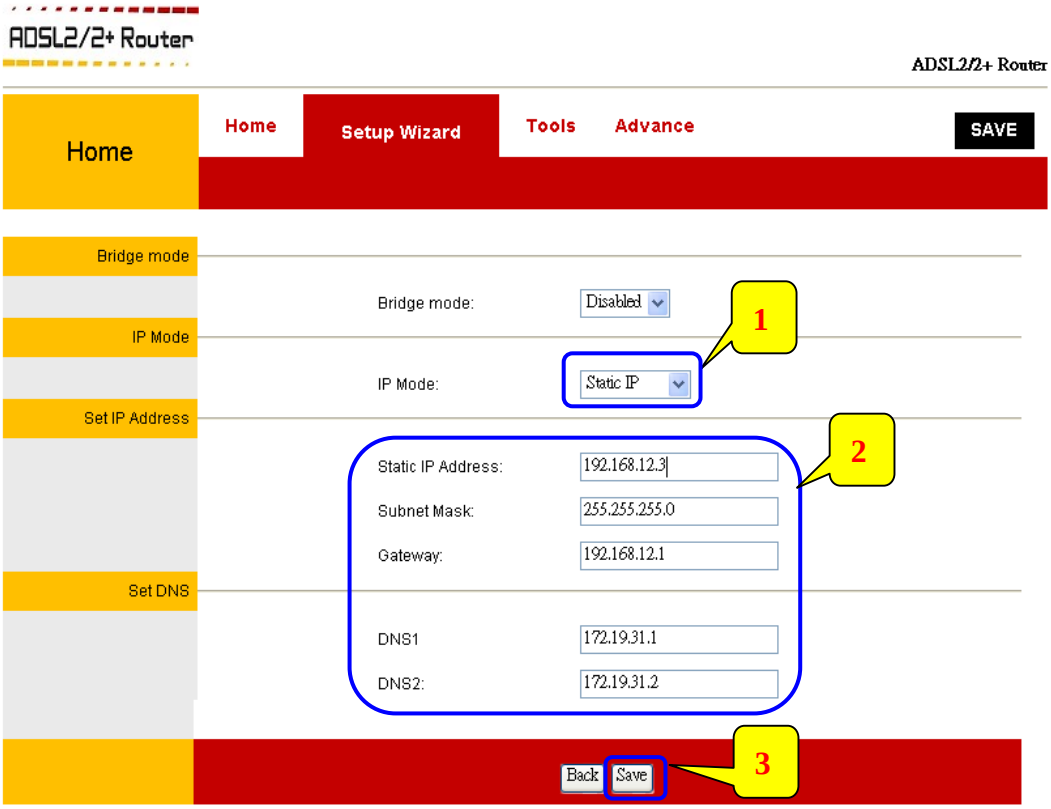
When **Bridge Mode** is set to **"Disabled"** (The default setting), please select **Dynamic IP** or **Static IP** from the **IP Mode** drop down manual.



- **Dynamic IP:** When **Dynamic IP** mode is selected, the following window's screen displays. Nothing to be filled under this mode. Just click the **"Save"** button to confirm your setting.



■ **Static IP:** When **Static IP** mode is selected from the **IP Mode** drop down manual, the following window's screen displays.



Manually enter the **"Static IP Address"**, **"Subnet Mask"**, **"Gateway"** and **"DNS"** which will be provided by your ISP.

☑ **Static IP Address:** This is the static IP Address given by the ISP.
Range for IP Address is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.

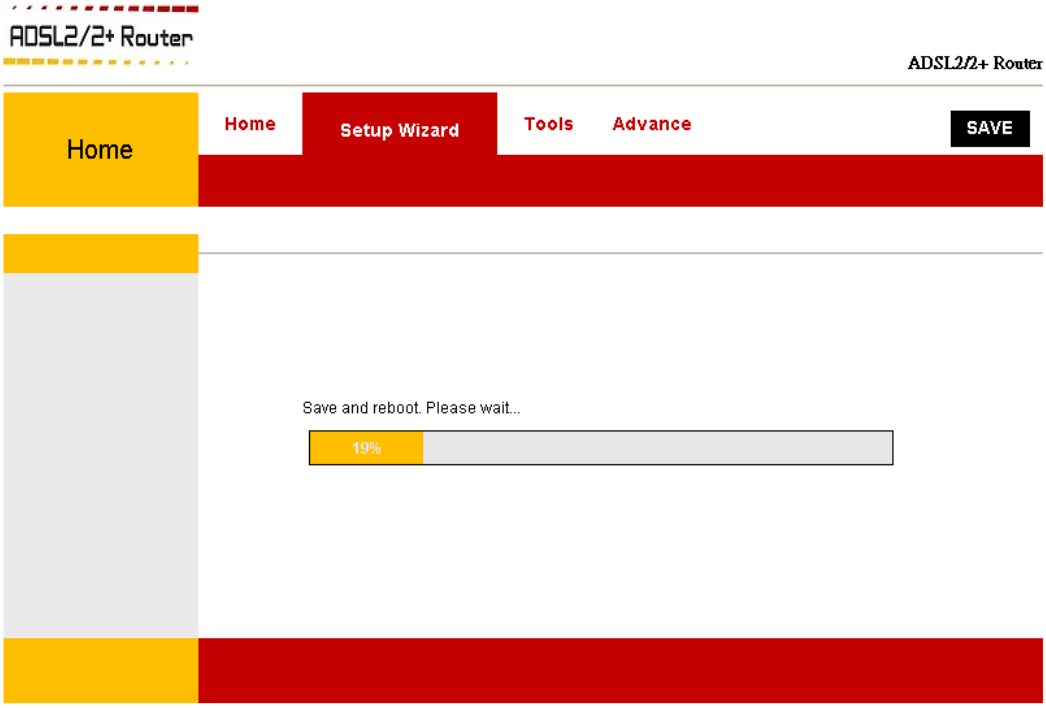
☑ **Subnet Mask:** This is the subnet mask provided by the ISP.
Range for Subnet Mask is x.x.x.x, where 0 ≦ x ≦ 255.

☑ **Gateway:** This is your gateway IP address.
Range for Gateway is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.

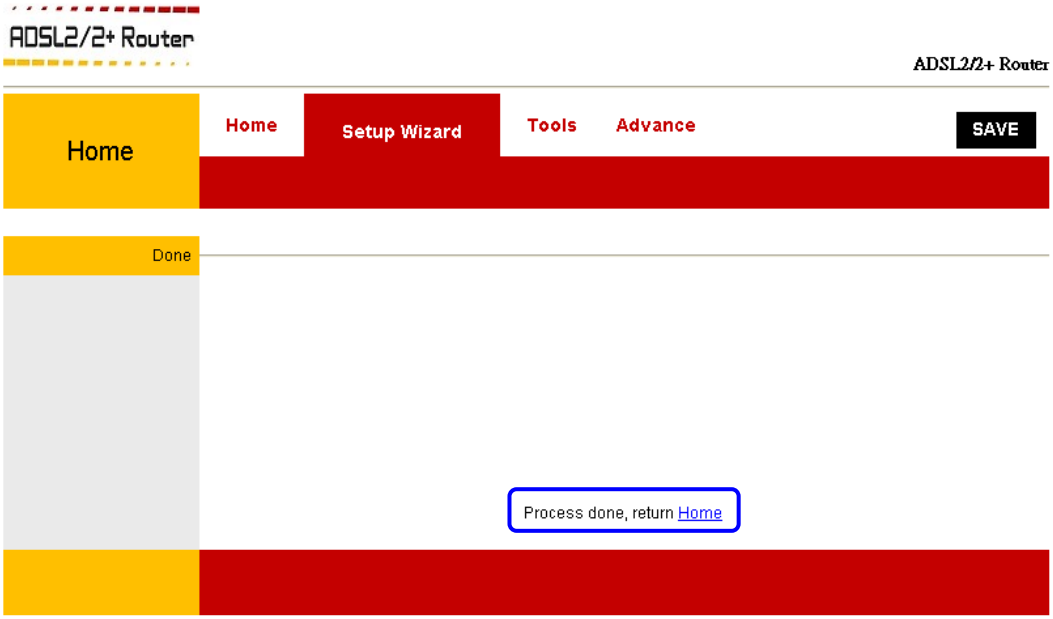
☑ **DNS:** This is the DNS address specify by the user or ISP. Check your ISP for setting detail.
Range for DNS Address is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.

Click the **"Save"** button after setup.

Click **"Save"** after setup. The following window display indicates the save setting process.



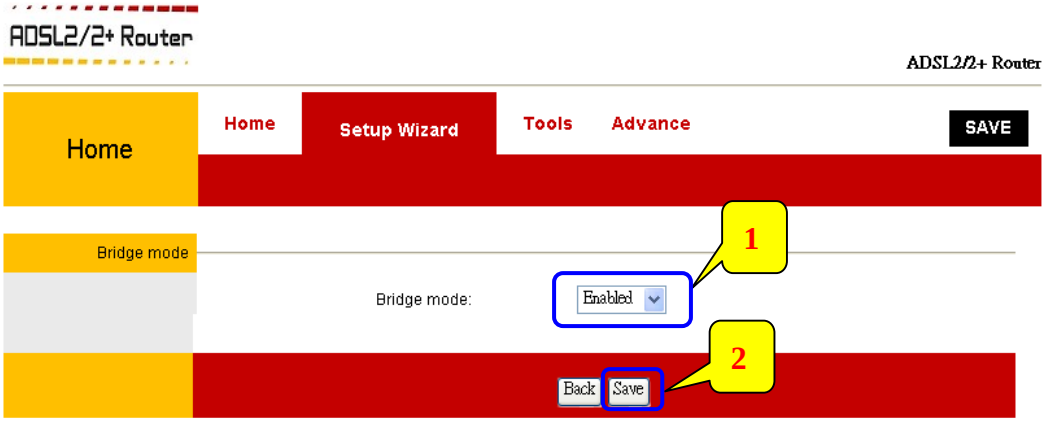
A **"Process Done"** screen will pop-up after the save setting process.



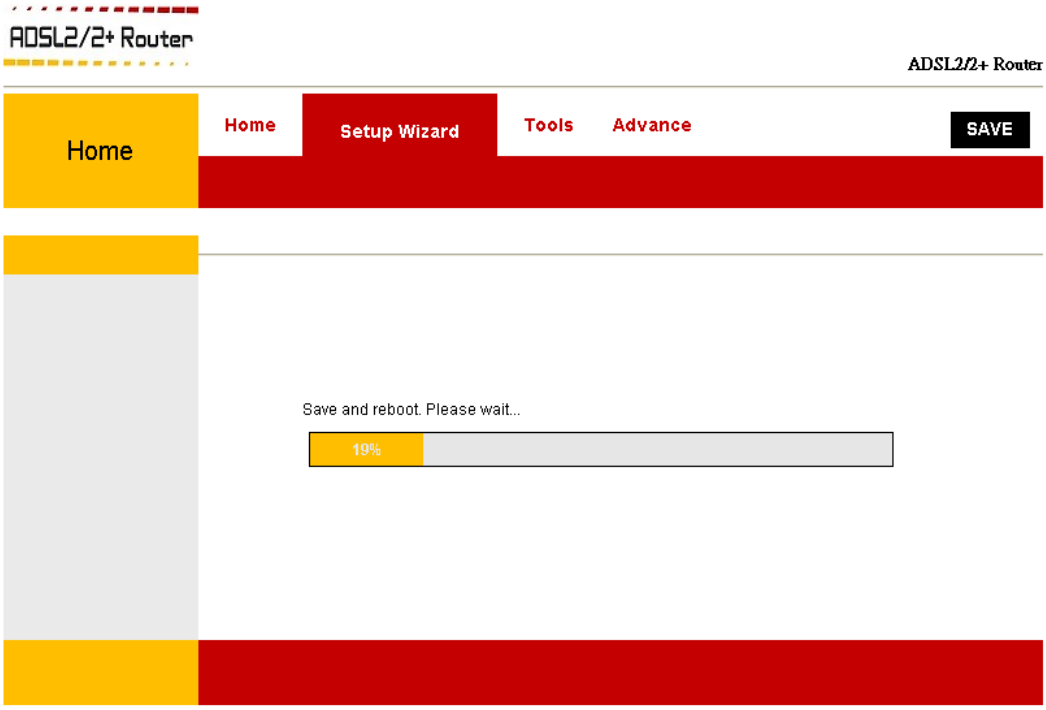
Click **"Home"** to return to the system Home page.

■ **Bridge Mode – Disabled (Default):**

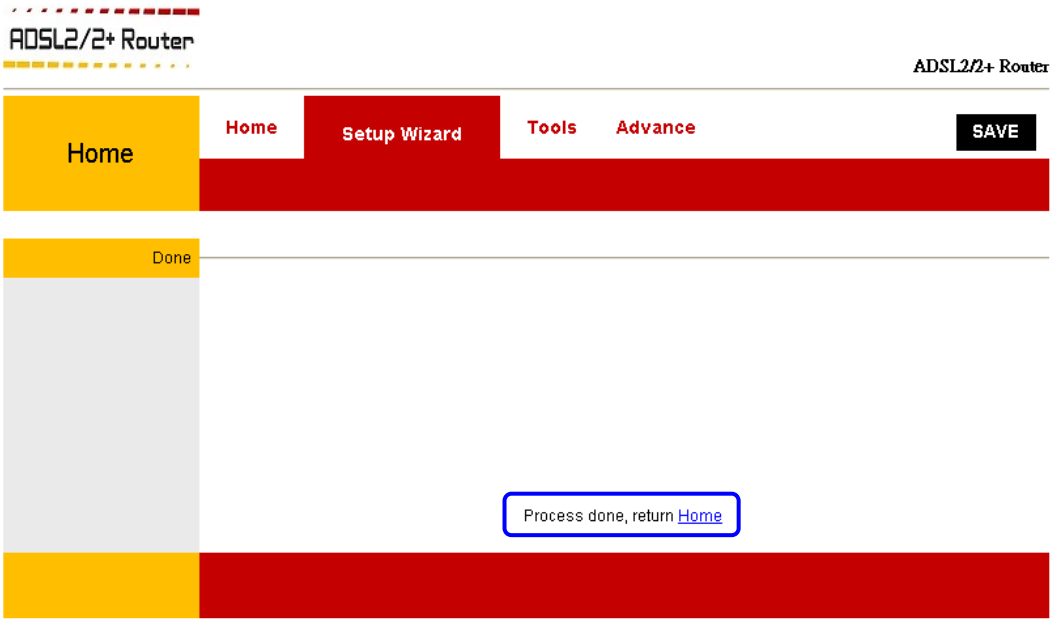
When **Bridge Mode** is set to **"Enabled"**, the following window's screen displays. Nothing to be filled under this mode.



Click **"Save"** after setup. The following window display indicates the save setting process.

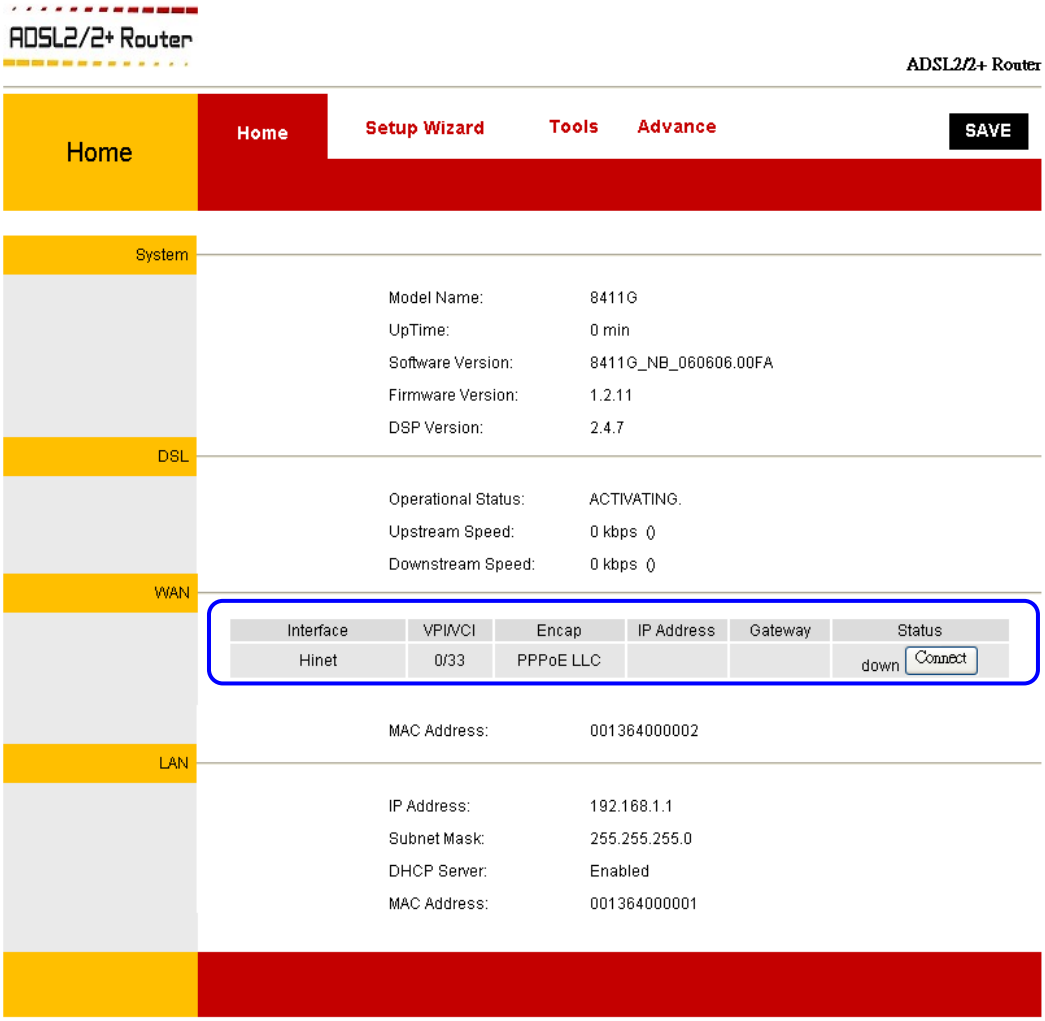


A **“Process Done”** screen will pop-up after the save setting process.



Click **“Home”** to return to the system Home page.

Step 2: The following configuration home page with the device setup information will pop-up after your confirmation at **Step 1**.



■ Check the following items when the above window pop-up. All the setting should be exactly the same with your setting at **STEP1**.

☑ **Interface:** Show the **ISP** name you'd selected in **STEP 1**.

☑ **VPI/VCI:** The **VPI/VCI** setting as shown in **STEP 1**.

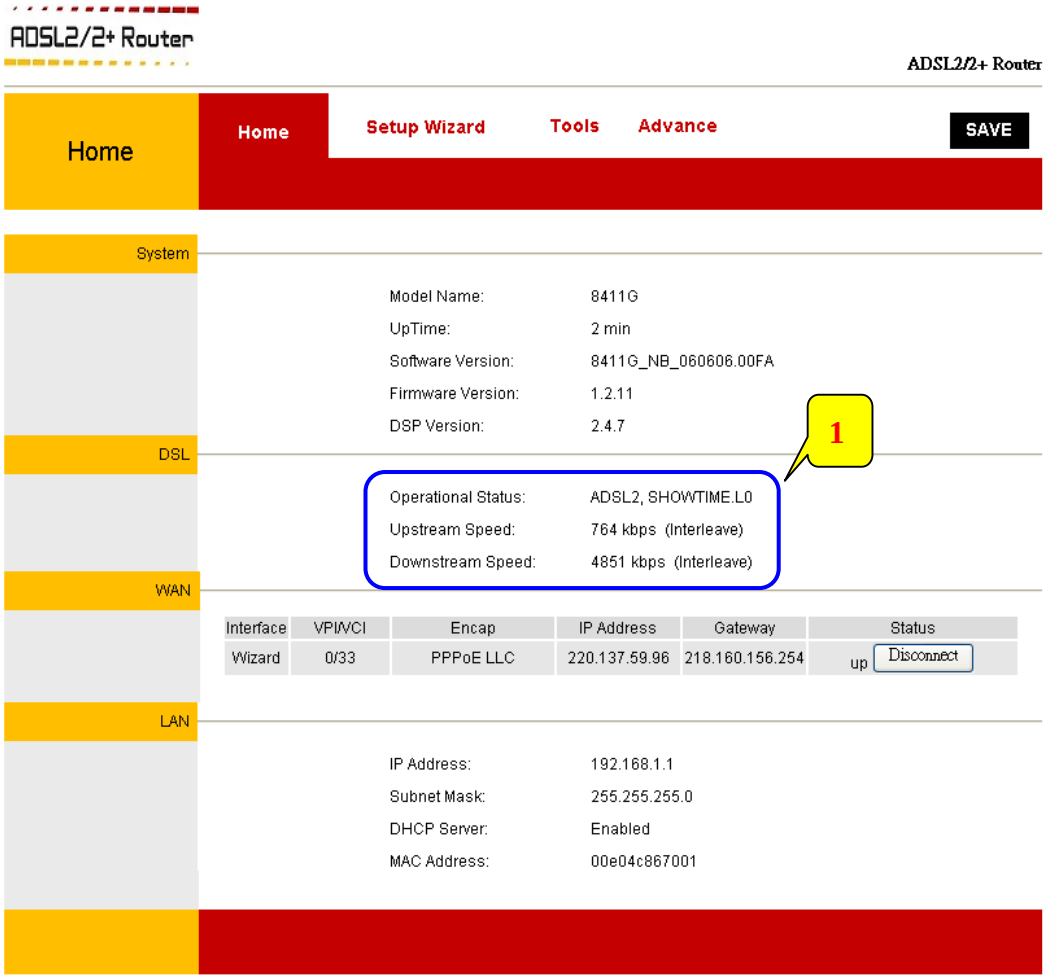
☑ **Encap:** Show the **Encapsulation** type selected in **STEP 1**.

NOTE: If the final setting are differ from what you'd selected in **STEP 1**, click **Setup Wizard** and redo the setup procedures or else check your dealer immediately for technical support.

Step 3: Under the system's **Home** page, check the **"DSL"** and **"WAN"** information.

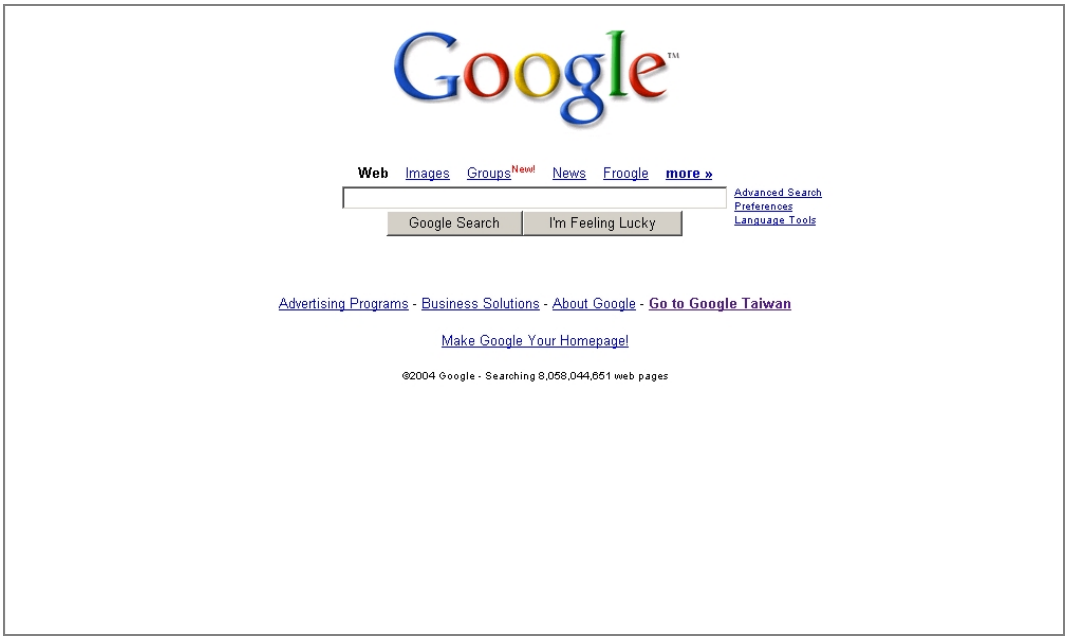
NOTE: The system **Home** page will refresh automatically every 10 seconds. You can also press the **"F5"** key on your keyboard to refresh the system **Home** page.

The **"Operational Status"**, **"Upstream Speed"** and **"Downstream Speed"** under **"DSL"** shows the real ADSL connection mode and connection speed in Kbps.



Step 4: Launch your web browser, and enter the Google Website Address: **"www.google.com"** in the address field then press **"Enter"**.

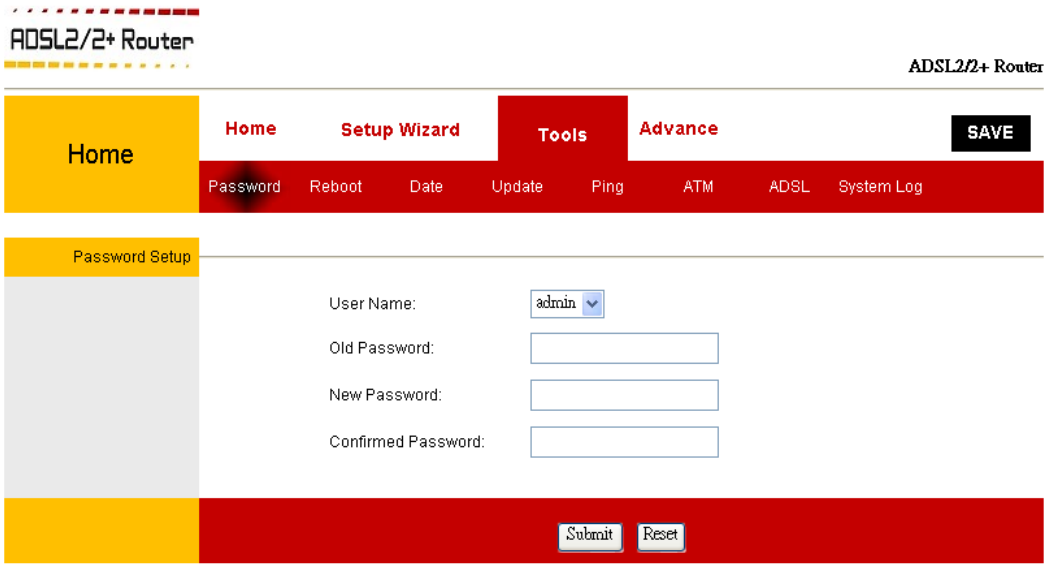
Step 5: The following Google website index page will display on your screen. This shows your ADSL connection is correctly set and access to the Internet is now available.



4.3 Tools

Figure below shows the **Tools** main screen, which can be accessed by clicking on the **Tools** tab from the top of the screen. This screen provides access to the following tools screens:

- ☑ Password
- ☑ Reboot
- ☑ Date
- ☑ Update
- ☑ Ping
- ☑ ATM
- ☑ ADSL
- ☑ System Log



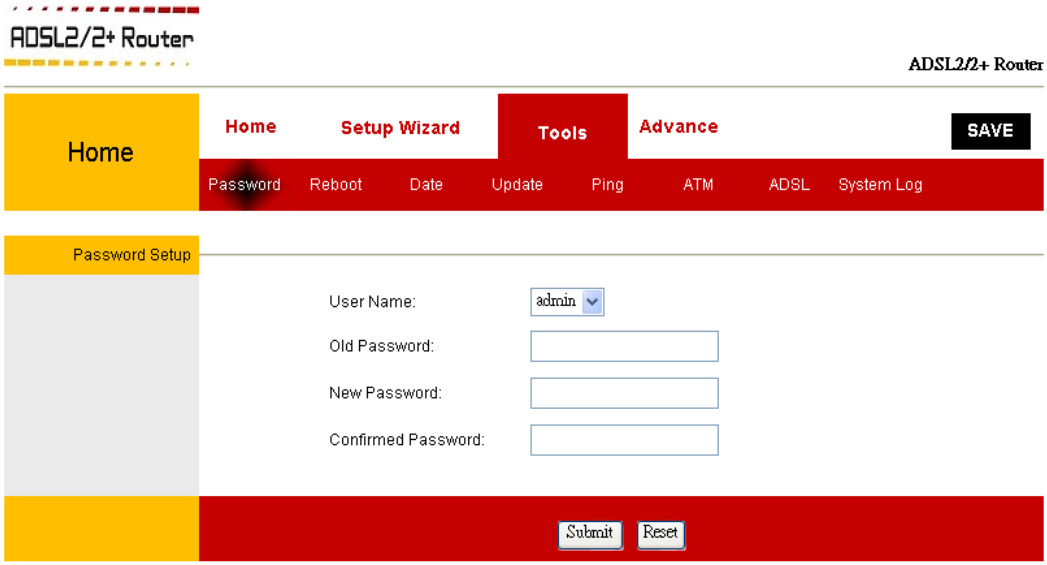
- **Password:** Configure user name and password.
- **Reboot:** Save your current 4 Ports 11g Wireless ADSL2/2+ Router's setting or reboot the device to it's default setting.
- **Date:** Configure the system Time Zone and system clock.
- **Update:** Upgrade the 4 Ports 11g Wireless ADSL2/2+ Router firmware.
- **Ping:** Run a ping test.
- **ATM:** Use to check weather the 4 Ports 11g Wireless ADSL2/2+ Router is properly connected to the WAN network.
- **ADSL:** Shows the ADSL Tone/Bit allocation when ADSL is successfully connected to your ISP.
- **System Log:** Display the 4 Ports 11g Wireless ADSL2/2+ Router's log.

4.3.1 Tools – Password

The **Password** page enables you to change your Password. It is recommended that you change the Password from the default **admin** to ensure the security of the 4 Ports 11g Wireless ADSL2/2+ Router.

For security reasons, the router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter the router User Name: **admin** and the router Password: **admin** to log in.

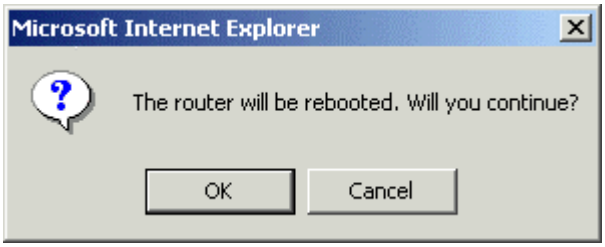
NOTE: If you forget your password, access to the 4 Ports 11g Wireless ADSL2/2+ Router can only be gained by resetting the unit to factory defaults. Pressing the **"Reset"** button for 10~15 seconds, the LED indicators will turns OFF and ON again indicates that the Reset process is successfully done.



- **User Name: "admin"** is your default user name. The User Name is unchangeable.
- **Old Password: "admin"** is your default password.
- **New Password:** Enter your new password here.
- **Confirmed Password:** Enter your new password here again to confirm your setting.
- **Submit:** Click **Submit** to complete your setting.
- **Reset:** Click **Reset** button and clear all your setting.
- **SAVE:** To permanently save your setting, click **SAVE** after clicking the **Submit** button.

Note: If you forget your password, you can press and hold the reset to factory default button for 10~15 seconds (or more). The 4 Ports 11g Wireless ADSL2/2+ Router will reset to its factory default configuration and all custom configuration will be lost.

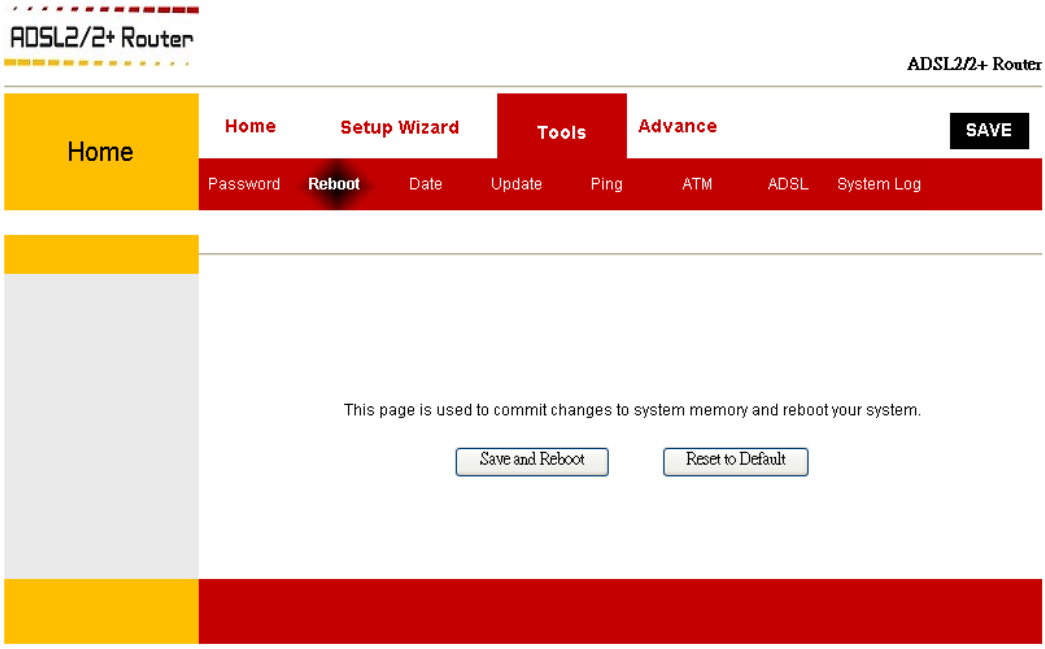
To complete and save the setting permanently, click **SAVE** after clicking the **Submit** button. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



Note: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

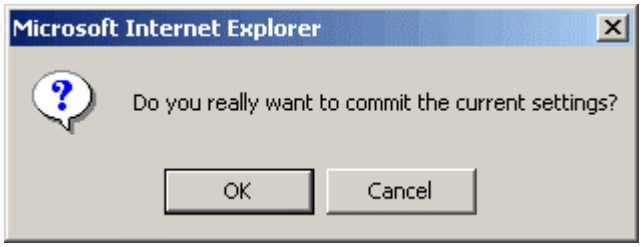
4.3.2 Tools – Reboot

Figure below shows the default **Reboot** screen. This page allows you to save the 4 Ports 11g Wireless ADSL2/2+ Router's configuration permanently, reboot the device and reset the device to its factory default setting.

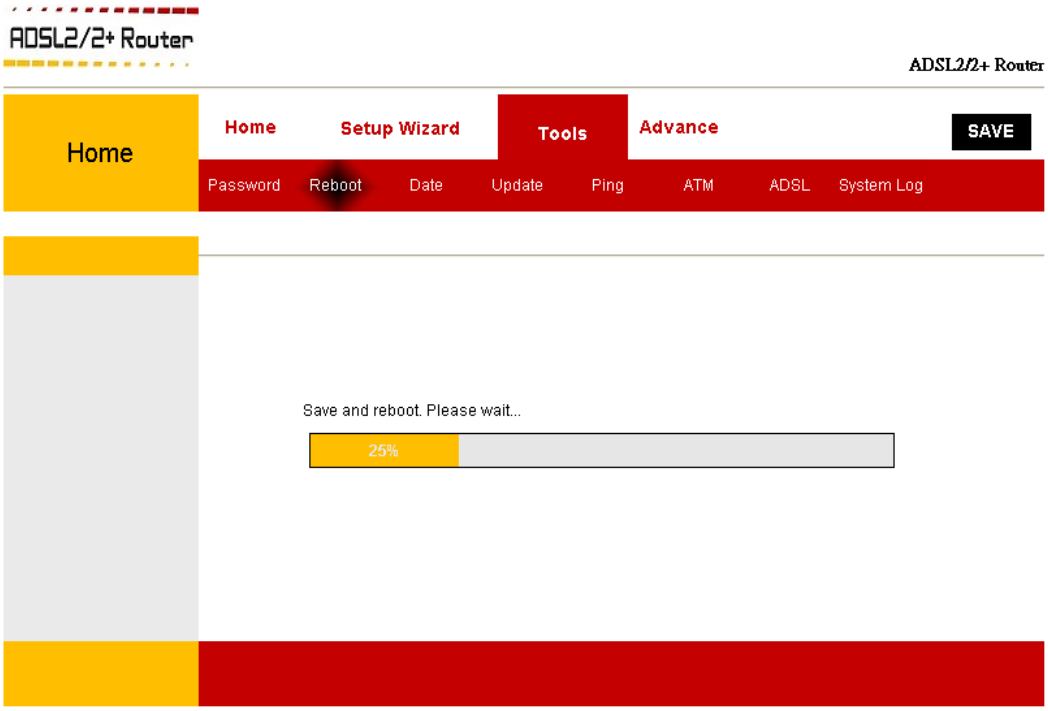


4.3.2.1 Reboot – Save and Reboot

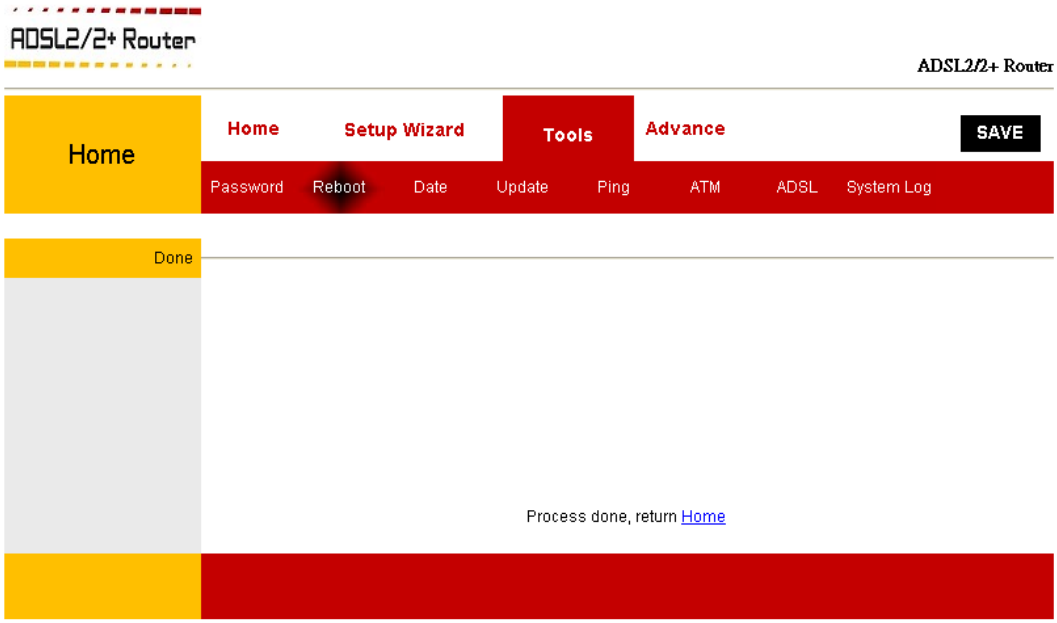
Press this button in order to permanently save the current configuration of the 4 Ports 11g Wireless ADSL2/2+ Router. The following wizard will pop-up when clicking the **"Save and Reboot"** button.



Click **"OK"** to confirm your setting. The following window display indicates the **"Save and Reboot"** process.

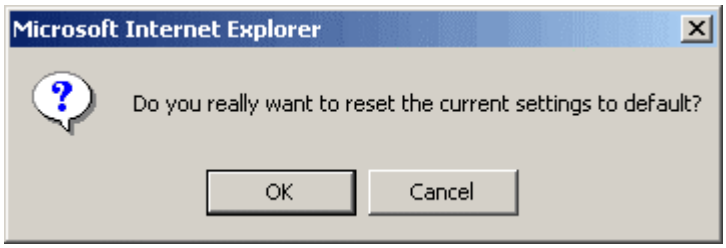


A **"Process Done"** screen will pop-up after the **"Save and Reboot"** process. Click **"Home"** to return to the system Home page.

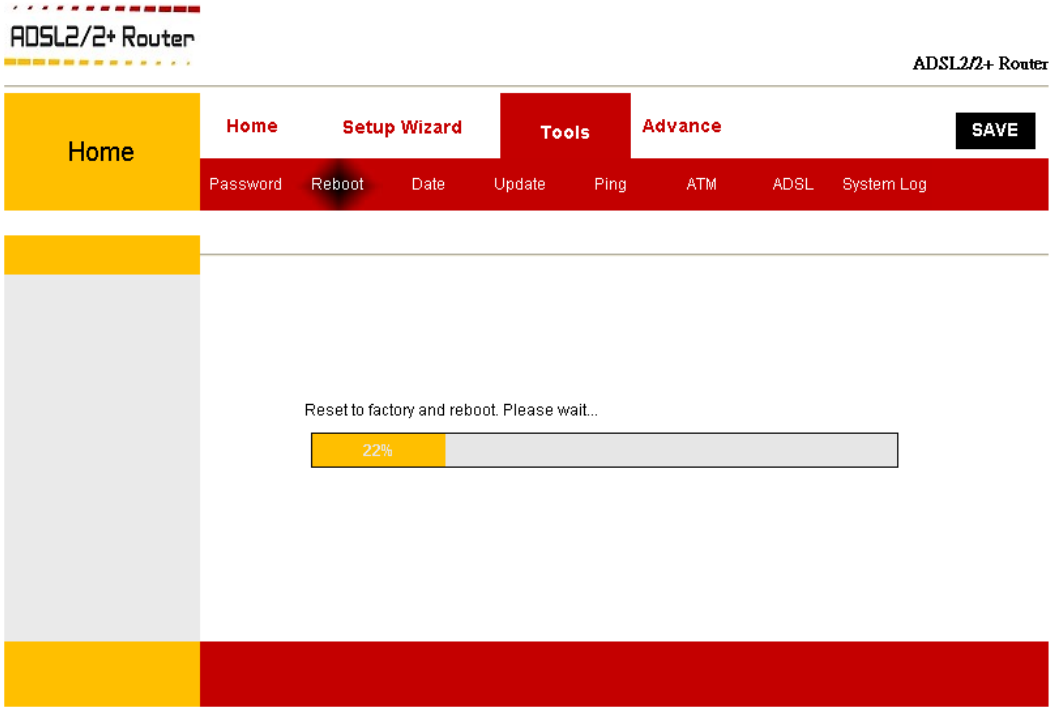


4.3.2.2 Reboot – Reset to Default

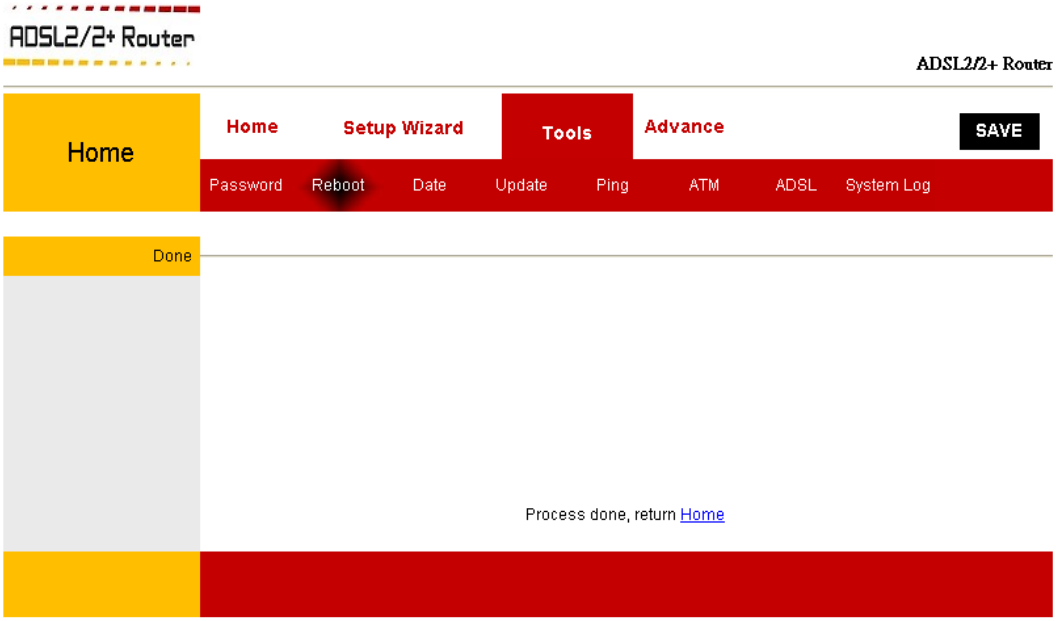
Press this button in order to restore factory default configurations.. The following wizard will pop-up when clicking the **"Reset to Default"** button.



Click **"OK"** to confirm your setting. The following window display indicates the **"Save and Reboot"** process.



A **“Process Done”** screen will pop-up after the **“Save and Reboot”** process. Click **“Home”** to return to the system Home page.

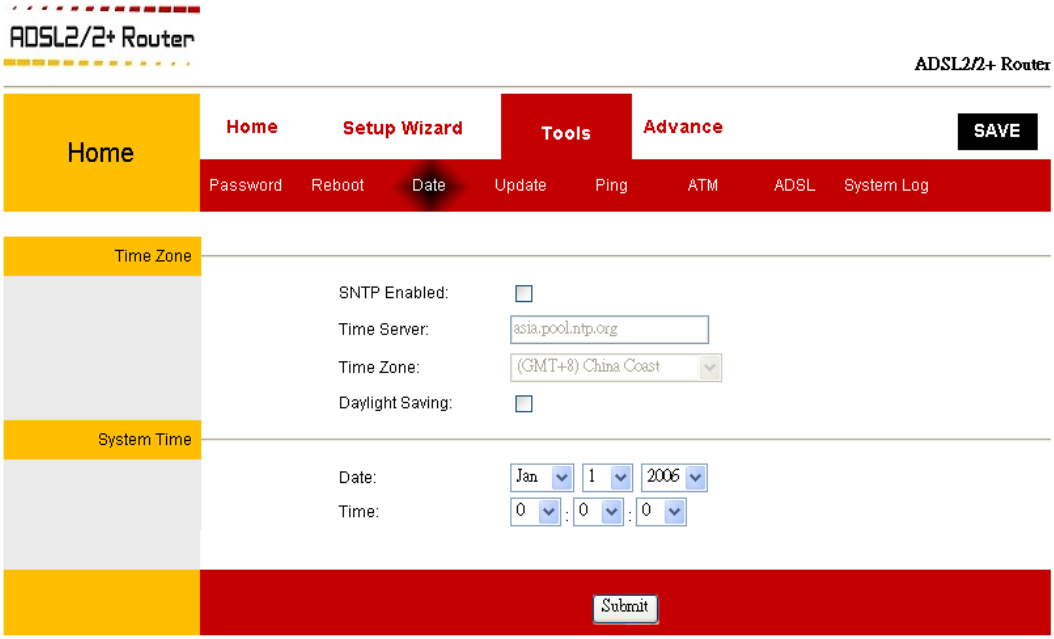


4.3.4 Tools – Date

You can set the system date and time manually or enable the SNTP feature so that the device acquires this information from an ISP server. Simple Network Time Protocol (SNTP) is an efficient method of obtaining the time from a Time Server.

When you set the date and time manually, the information will be held only as long as the device stays on; if power is turned off or you reboot, the date and time revert to default values and must again be updated.

When you enable SNTP (Simple Network Time Protocol), the device connects to an ISP server that provides the date and time information. You cannot use Configuration Manager to specify the IP address of this server; it must have been included as a pre-configured software setting. Verify with the ISP that they have provided an SNTP server address in the configuration before enabling this service.



- **SNTP:** To enable SNTP, click the Enable radio button. The remaining date and time fields will be dimmed (unavailable for entry).
- **Time Server:** This is the time server from which the 4 Port 11g Wireless ADSL2/2+ Router retrieves the time.
- **Time Zone:** This specifies the time zone (Geographical location).
- **Daylight Saving:** If you are setting the date and time manually, you can select your time zone from the drop-down list, and then click the appropriate radio button to indicate whether Daylight Savings Time is currently in effect. After you initially set the time, turning Daylight Saving Time **ON** (Enabled) or **OFF** (Disabled) will adjust the current displayed time by one hour in the appropriate direction..
- **Date and Time:** To set the date and time manually, ensure that the **SNTP** field is set to **Disable**. Click the date and time check boxes to select the appropriate values from the drop-down lists. The time displays in military format.

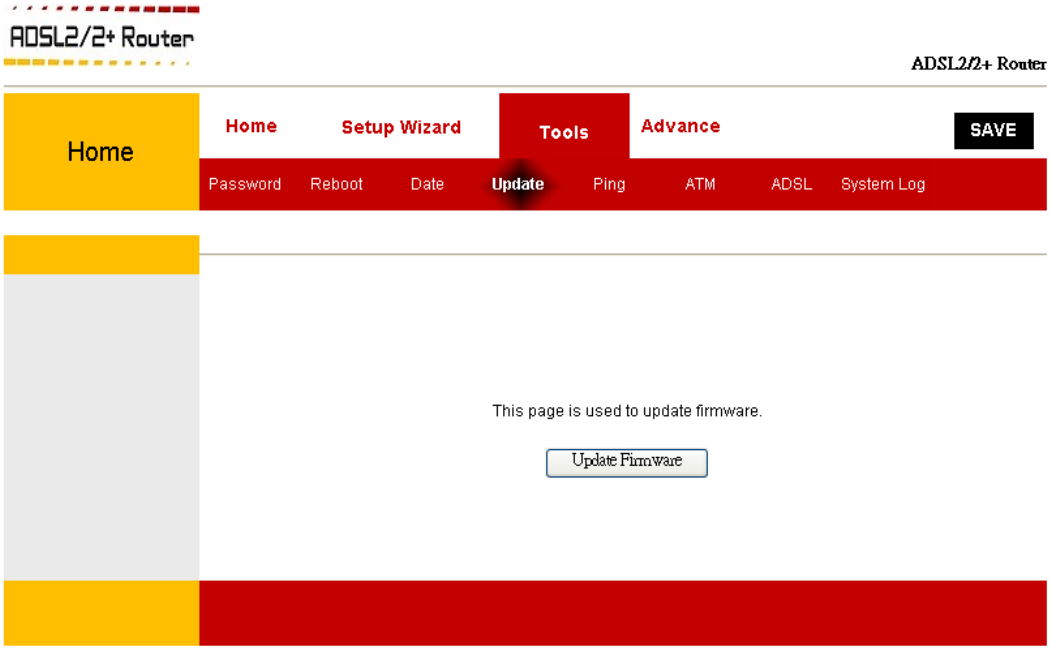
Follow these instructions to change the system date and time or enable SNTP:

1. To enable **SNTP**, click the Enable radio button. The remaining **Date** and **Time** fields will be dimmed (unavailable for entry).
2. Click to enable Daylight Saving functionality (Optioanl).
3. **Date & Time:** To set the date and time manually, ensure that the **SNTP** field is set to **Disable** (Uncheck). Click the date and time check boxes to select the appropriate values from the drop-down lists. The time displays in military format.
4. Click **"Submit"** after setup.
5. To complete and save the setting permanently, click **SAVE** after clicking the **Submit** button.

4.3.5 Tools – Update

Firmware is the software that controls the 4 Ports 11g Wireless ADSL2/2+ Router and also provides the user interface that is subject of this manual. The Firmware resides in the 4 Ports 11g Wireless ADSL2/2+ Router internal Flash memory; currently loaded firmware version can be found under **Home → System**.

To access Firmware Updates, click on **Tools → Update**. The following window screen will pop-up.



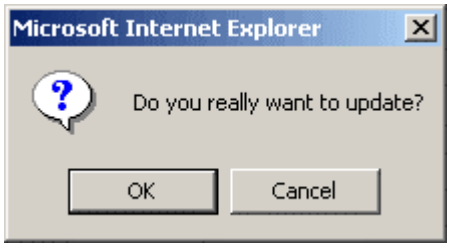
- **Update Firmware:** Click the **Update Firmware** button to upgrade your 4 Ports 11g Wireless ADSL2/2+ Router. The system will be restarted automatically after the Firmware/Image is successfully uploaded. You will need to reconnect again to configure your setup.

Note: When uploading Firmware/Configuration File to the 4 Ports 11g Wireless ADSL2/2+ Router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the upgrading process. When the upload is complete, your 4 Ports 11g Wireless ADSL2/2+ Router will automatically reboot and restart. The upgrade process will typically take about 3~4 minutes.

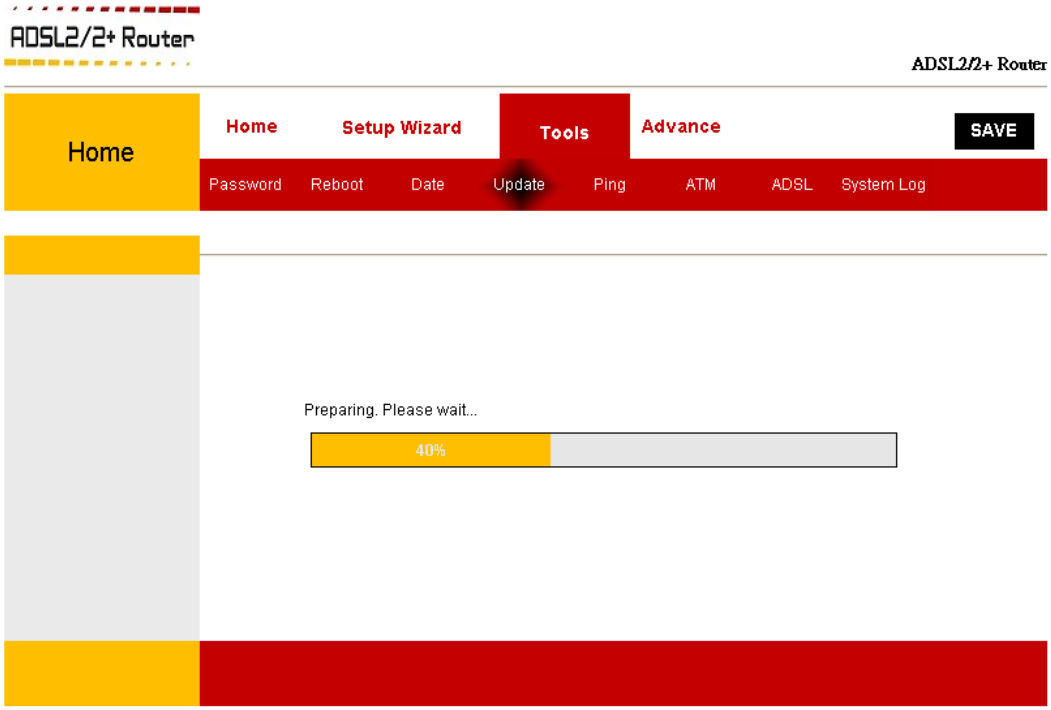
4.3.5.1 Update Procedure

Use the following procedures to update firmware for your 4 Ports 11g Wireless ADSL2/2+ Router.

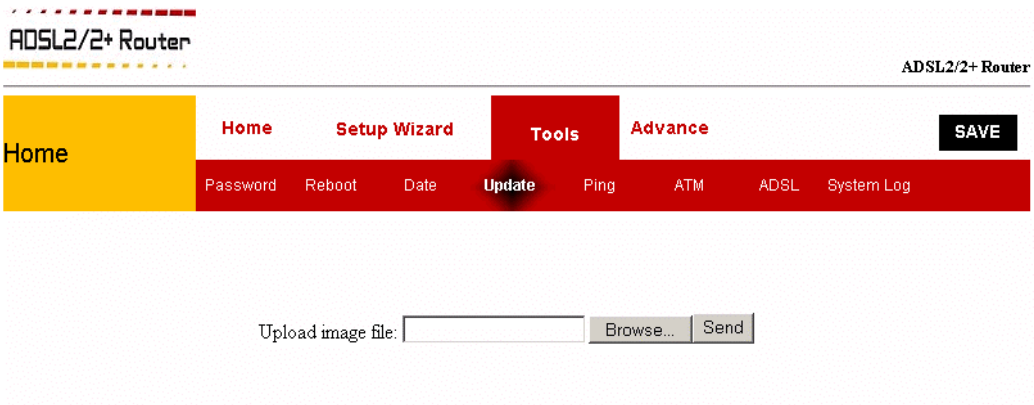
1. Click **Tools – Update** to upgrade your 4 Ports 11g Wireless ADSL2/2+ Router's firmware. The following wizard will pop-up. Click **"OK"** to confirm your changes.



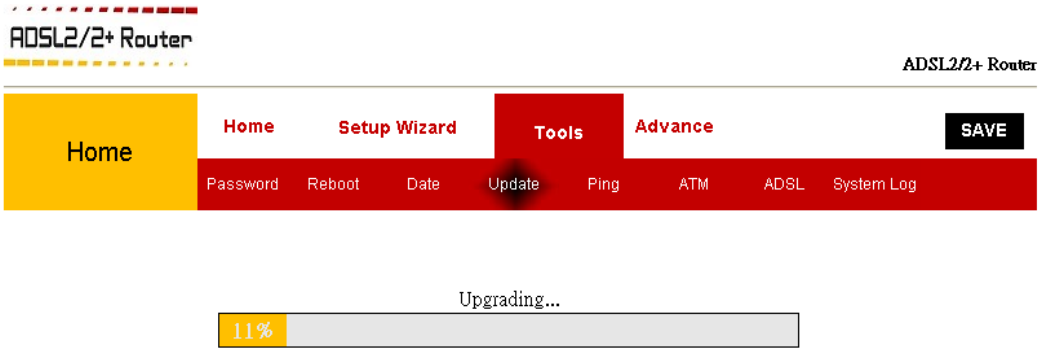
The following upgrade preparing screen will pop-up.



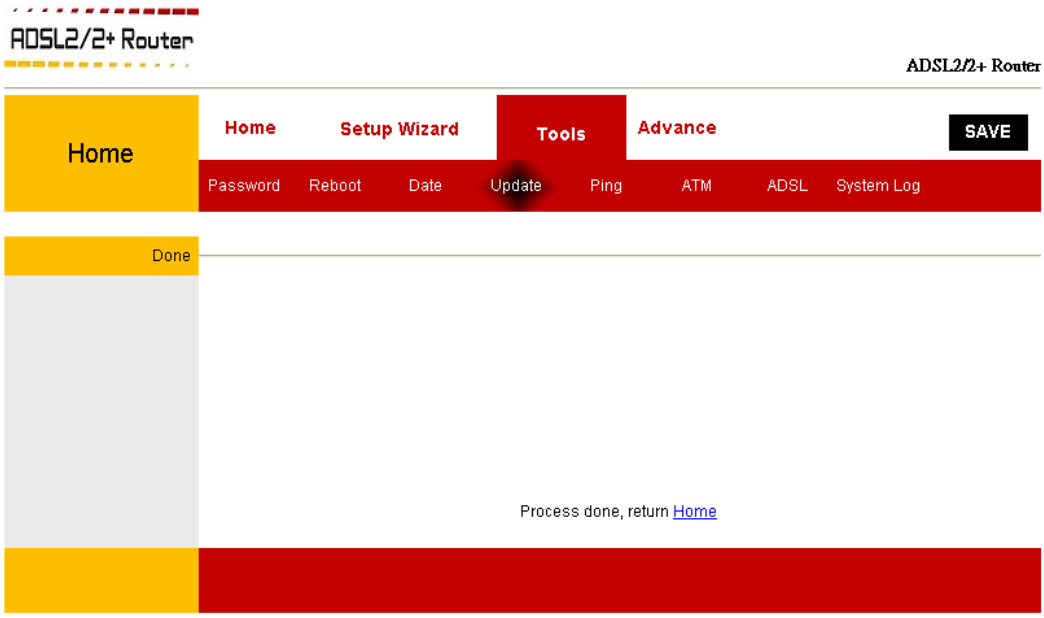
2. The following screen display. Click **Browse** and select the file to update. The file name will appear in the Select a File field.



3. Click **Send** after setup. The status of the uploading process display.



4. When the uploading process finished, the following complete notice screen will display. Click the **"Home"** button and log back to the system Home page.

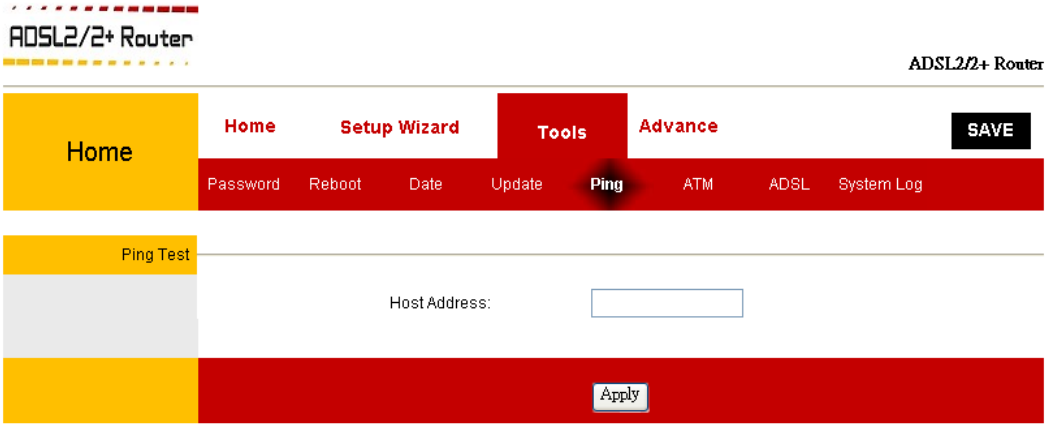


5. If you want to make sure the firmware is properly upgraded, go to **Home → System** and check on the Firmware and Software version information on the System Information screen

4.3.6 Tools – Ping

Once you have your 4 Ports 11g Wireless ADSL2/2+ Router configured, it is a good idea to make sure you can Ping the network.

Figure below shows the default Ping Test screen, which can be accessed by clicking on the Ping Test link from the Tools screen. If you have your PC connected to the 4 Ports 11g Wireless ADSL2/2+ Router via the default DHCP configuration, you should be able to Ping the network address 192.168.1.1. If the pings for both the WAN side and the LAN side are complete, and your have the proper protocol configures, you should be able to surf the Internet.



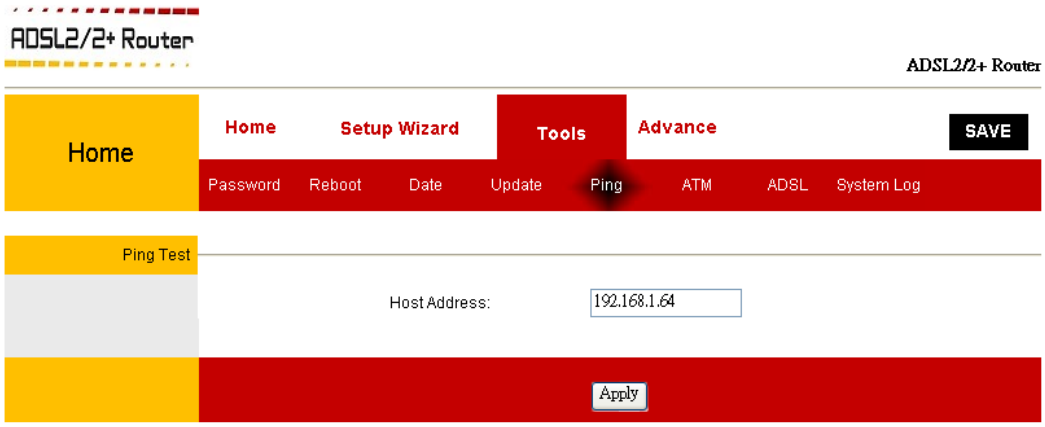
- **Host Address:** Enter the IP address that you want to ping.

- **Apply:** Click **Apply** to start the ping test. The result will be shown in the window underneath.

4.3.6.1 Ping Test Procedure

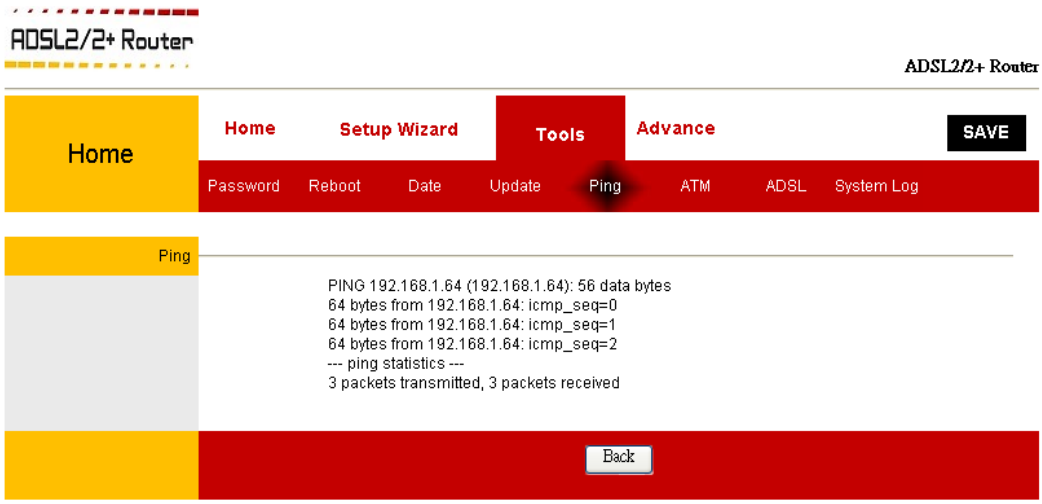
1. Click **Ping** from the **Tools** menu to access the Ping Test screen.

2. Enter the Host IP Address to ping



3. Click **Apply** button to start the Ping process.

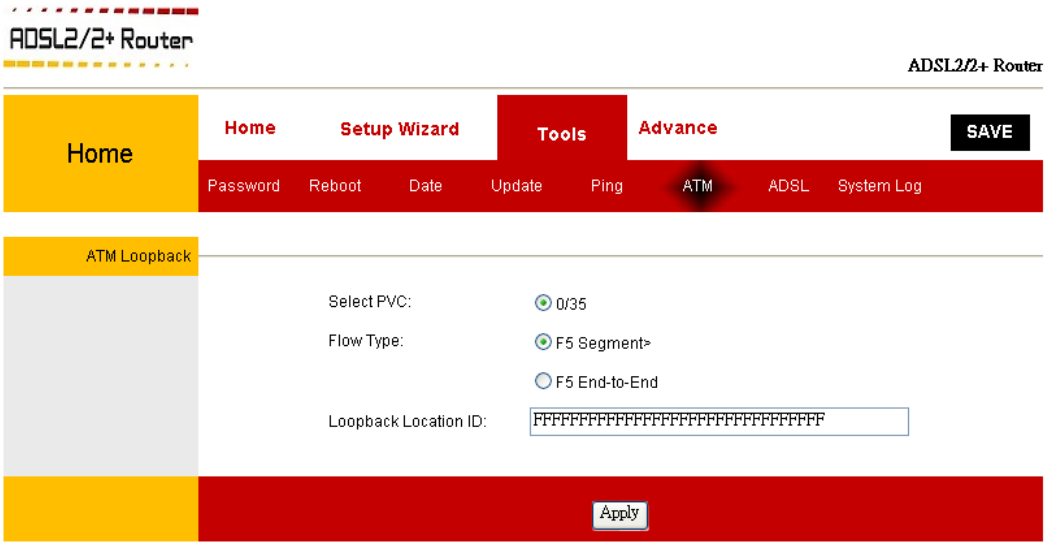
4. The ping results will be displayed in the box on the screen. If the ping test was successful, it means that the TCP/IP protocol is up and running. If the Ping test failed, the TCP/IP protocol is not loaded for some reason, you should restart the 4 Ports 11g Wireless ADSL2/2+ Router.



5. Click **Back** button and return to the Ping home page.

4.3.7 Tools – ATM

The **ATM** Test is used to check weather your 4 Ports 11g Wireless ADSL2/2+ Router is properly connected to the WAN network. This test may take a few seconds to complete. Before running this test, make sure you have at least one WAN connection configured and have valid ADSL link; if the ADSL link is not connected, the test will fail.



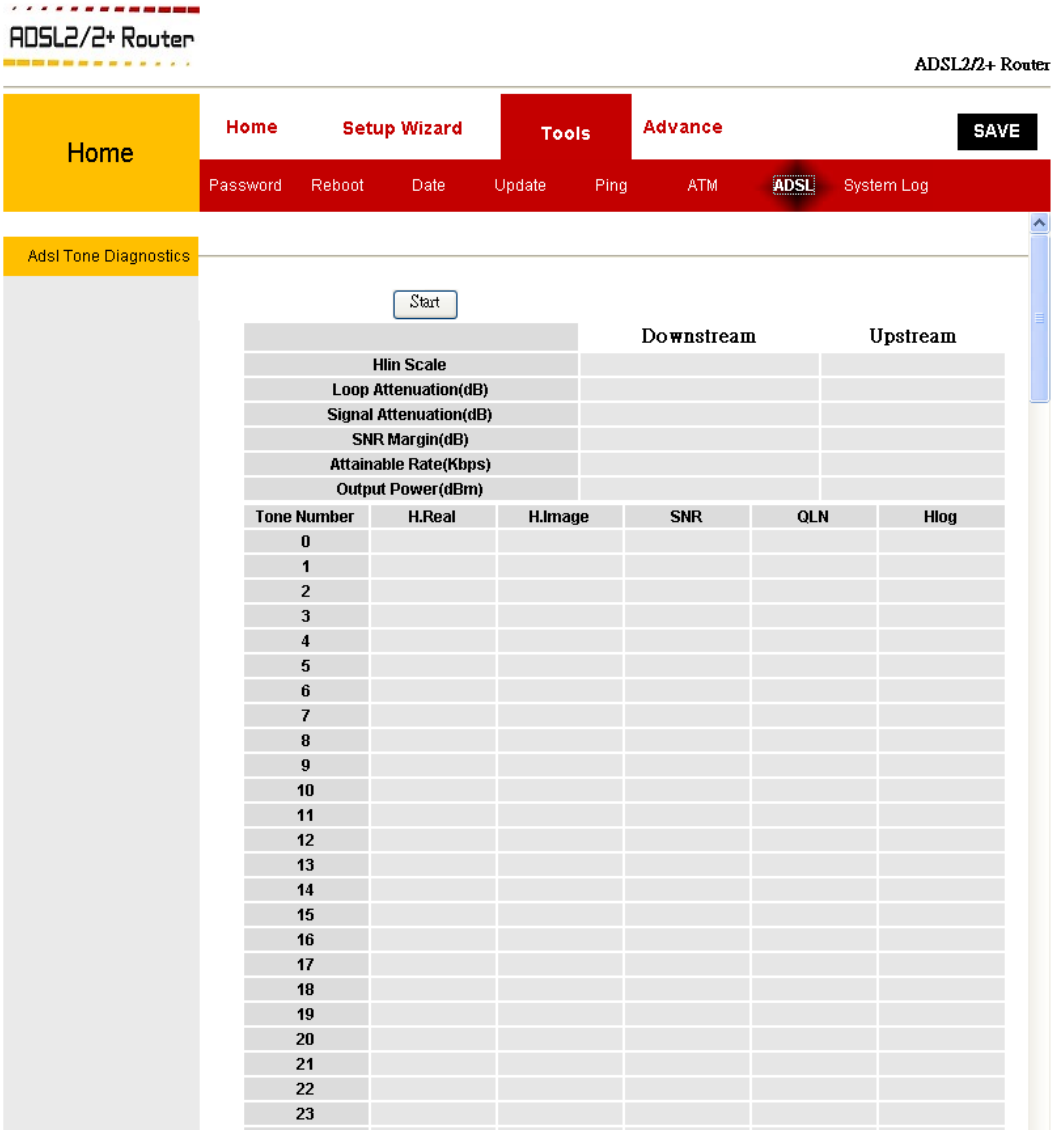
- **Select PVC:** Virtual Path identifier/Virtual Channel Identifier.

- **Flow Type:** There are 2 test types:
  - ☑ **F5 Segment:** F5 segment.
  - ☑ **F5 End-to-End:** F5 end to end.

- **Loopback Location ID:** Display the Loopback Location ID.

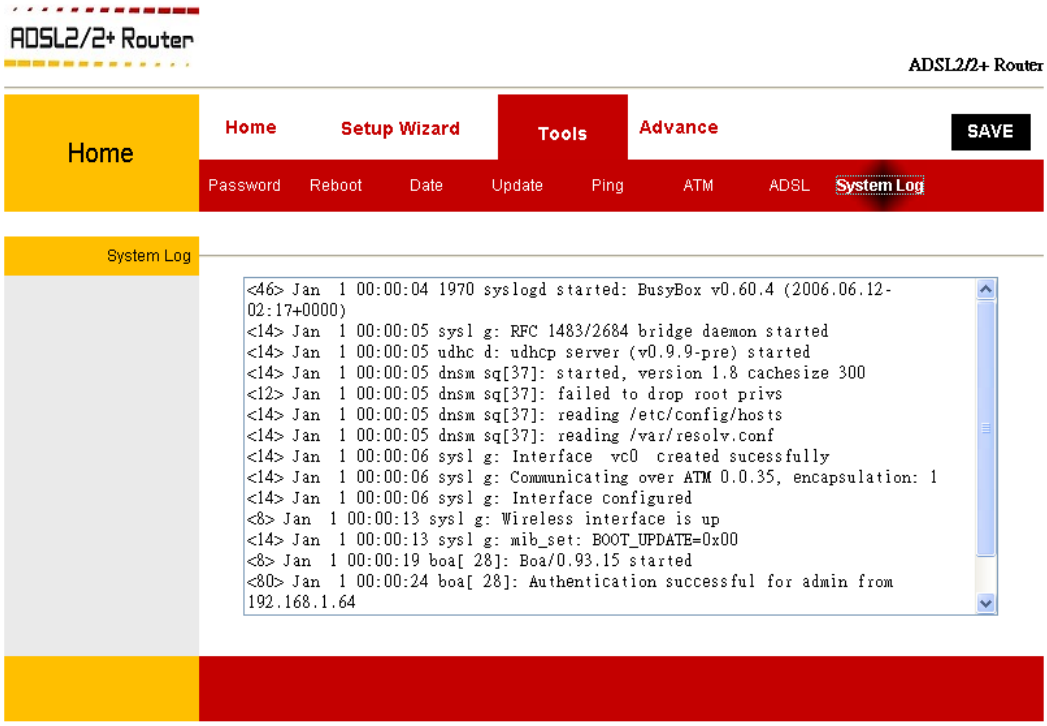
4.3.8 Tools – ADSL

The **ADSL** page shows the ADSL physical layer or link status. The information displayed on this page is either inherent to the 4 Port 11g Wireless ADSL2/2+ Router or set by the ADSL Central Office (CO) DSLAM, neither of which cannot be changed by the user. This page contains information that is dynamic and will refresh every 5 seconds.



4.3.9 Tools – System Log

You can display your 4 Ports 11g Wireless ADSL2/2+ Router's log by clicking on the **System Log** link from the **Tools** Main screen. The **System Log** screen allows you to view all logged information. Depending upon the severity level, the logged information will generate log reports to a remote host (if remote logging is enabled). This page contains information that is dynamic and will refresh every 5~10 seconds.



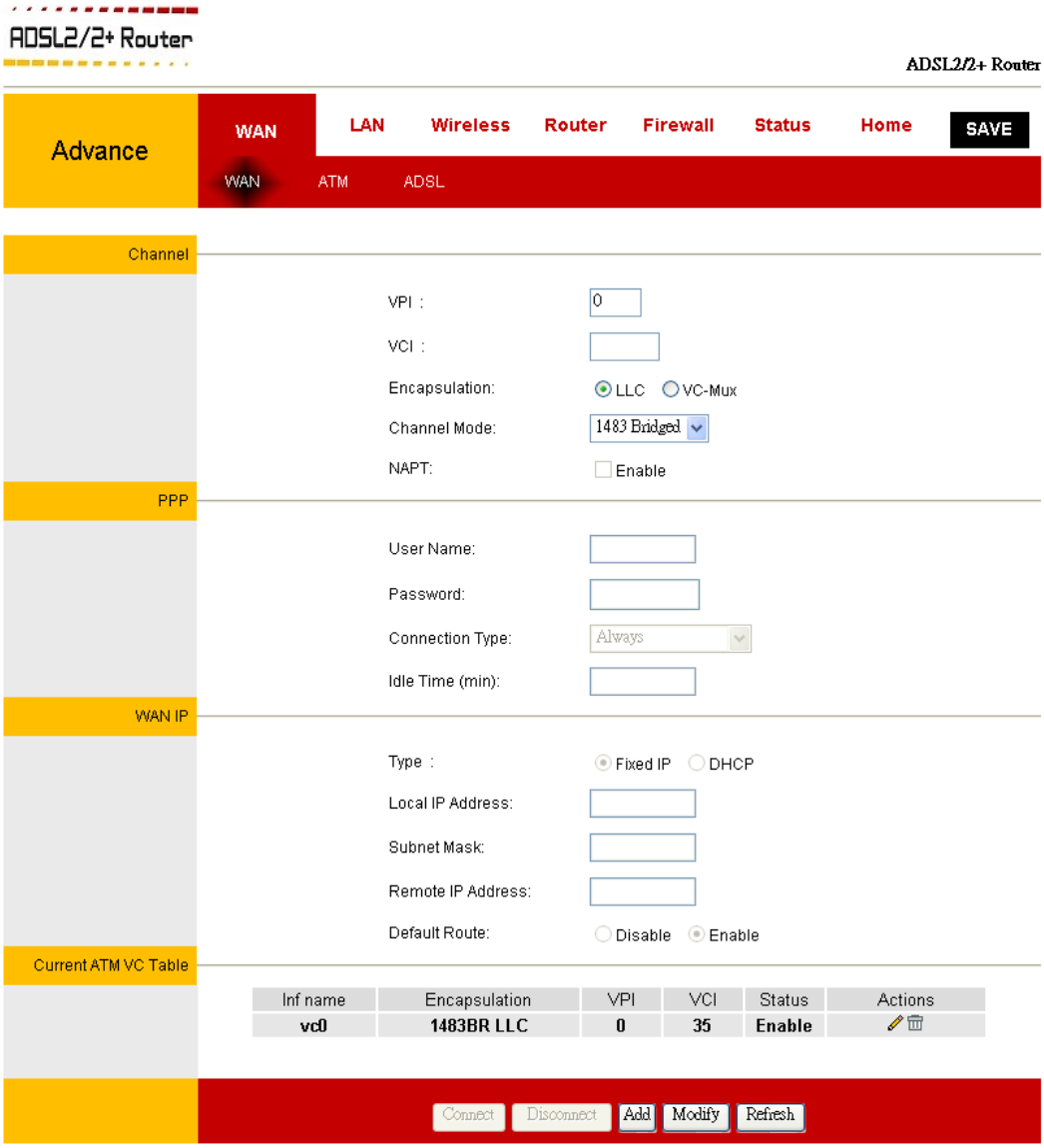
4.4 Advance

The Advanced Menu provides access to advanced networking, management and routing capabilities. Click the **Advance** tab and the following screen will pop-up.

The **Advance** tab allows you to perform advanced configuration functions for existing connections including:

- Enabling and disabling of key features including SNTP, SNMP, IP QoS, RIP, Access Control, TR-069, TR-068 and multicasting.
- Management of LAN port interfaces, packet flow, isolation and filtering.
- Management of WAN port interface, ADSL protocols management and creating new connection.
- Configure the Wireless Access setting, Security and Management.
- Showing the details of the network statistics.

At least one WAN connection must be configured before implementing advanced WAN configuration features. At least on LAN group must be defined before implementing advanced LAN configuration features.

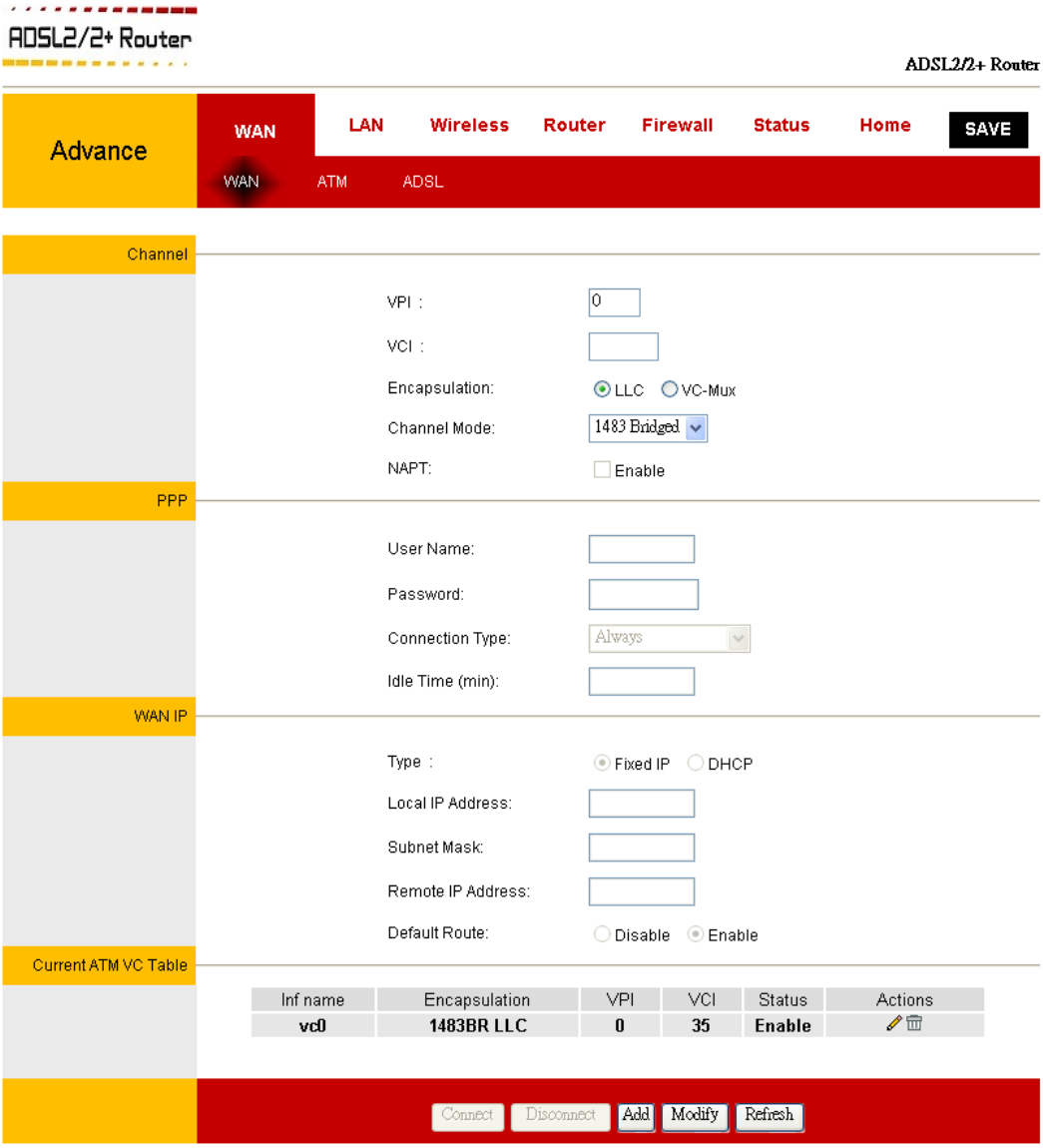


4.4.1 Advance – WAN

Figure below shows the **Advance** main page, which is accessed by clicking the **Advance** tab at the top of the page.

The **Advanced – WAN** configuration page shows you the device modulation type and making/creating new **WAN** connection profile.

The devices WAN-side interfaces are used to communication via the ADSL port. A WAN interface comprises two layers: a lower-level interface and a higher-level protocol interface. The **WAN** interface enables the device to communicate using the Asynchronous Transfer Mode protocol. The ATM protocol provides a common format for transmitting data over a variety of hardware systems that make up the backbone of the Internet.



- **Channel:**
  - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an 8-bit field in the ATM cell header. The VPI field specifies this 8-bit identifier for routing. Range for VPI field is 0 ~ 255.
  - ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination. Range for VCI field is 0 ~ 65535.
  - ☑ **Encapsulation:** Determines the type of data link used to communicate with your ISP. This 4 Ports 11g Wireless ADSL2/2+ Router support **LLC** and **VC-Mux** encapsulation type.
  - ☑ **Channel Mode:** The type of protocol used. Your ISP may use PPPoE, PPPoA, 1483 Bridged, 1483 Routed or 1483 MER connection type.
  - ☑ **Enable NAPT:** Click **"Enable"** or **"Disable"** the NAPT functionality. The **NAPT** translates private source IP addresses to a single public IP address.

- **PPP (For PPPoE and PPPoA Connection Type):**
  - ☑ **User Name:** Enter your User Name which will be provided by your ADSL ISP.
  - ☑ **Password:** Enter your Password which will be provided by your ADSL ISP.
  - ☑ **Connection Type:** Select the ADSL connection mechanism.
  - ☑ **Idle Time:** Set the Idle Time up.

- **WAN IP (For 1483 Routed & 1483 MER Connection Type):**
  - ☑ **Type:** Click to select **"Fixed IP"** or **"DHCP"** connection type.
  - ☑ **Local IP Address:** The IP Address provided by your ADSL ISP.
  - ☑ **Subnet Mask:** The Subnet Mask Address provided by your ADSL ISP.
  - ☑ **Remote IP Address:** The Gateway Address of your 4 Ports 11g Wireless ADSL2/2+ Router.
  - ☑ **Default Route:** Click to **"Enable"** or **"Disable"** Default Route.

- **Current ATM VC Table:**
  - ☑ **Inf Name:** The name of the lower-level interface on which this connection operates.
  - ☑ **Encapsulation:** The Encapsulation type used by your ADSL ISP.
  - ☑ **VPI/VCI:** The VPI/VCI setting of your ADSL ISP.
  - ☑ **Status:** The current connection status.
  - ☑ **Action:** Edit/Delete your current connection profile.

- **Add:** Adding New Connection profile.
- **Modify:** Modify existing connection profile.
- **Reset:** Reset or clear all your current setting.
- **Refresh:** Click Refresh to redisplay the page.

4.4.1.1 Creating WAN Connection

Before the 4 Ports 11g Wireless ADSL2/2+ Router will pass any data between the LAN interface(s) and the WAN interface, the WAN side of the modem must be configured. Depending upon your ADSL service provider or your ISP, you will need some (or all) of the information outlined below before you can properly configure the WAN:

- Your ADSL account Username and Password
- Your ADSL line VPI and VCI setting
- Your ADSL encapsulation type or multiplexing (Either LLC or VC. Check your ISP for detail)
- Your ADSL Training Mode or Handshaking Mode (default is MMODE)

For **PPPoA** or **PPPoE** users, you also need these values from your ISP:

- Your account Username
- Your account Password

For **RFC 1483** users, you may need these values from your ISP:

- Your ADSL fixed Internet IP address
- Your Subnet Mask
- Your Default Gateway address
- Your primary DNS IP address

Since multiple users can use the 4 Ports 11g Wireless ADSL2/2+ Router, the 4 Ports 11g Wireless ADSL2/2+ Router can simultaneously support multiple connection types; hence, you must set up different profiles for each connection. The 4 Ports 11g Wireless ADSL2/2+ Router supports the following protocols:

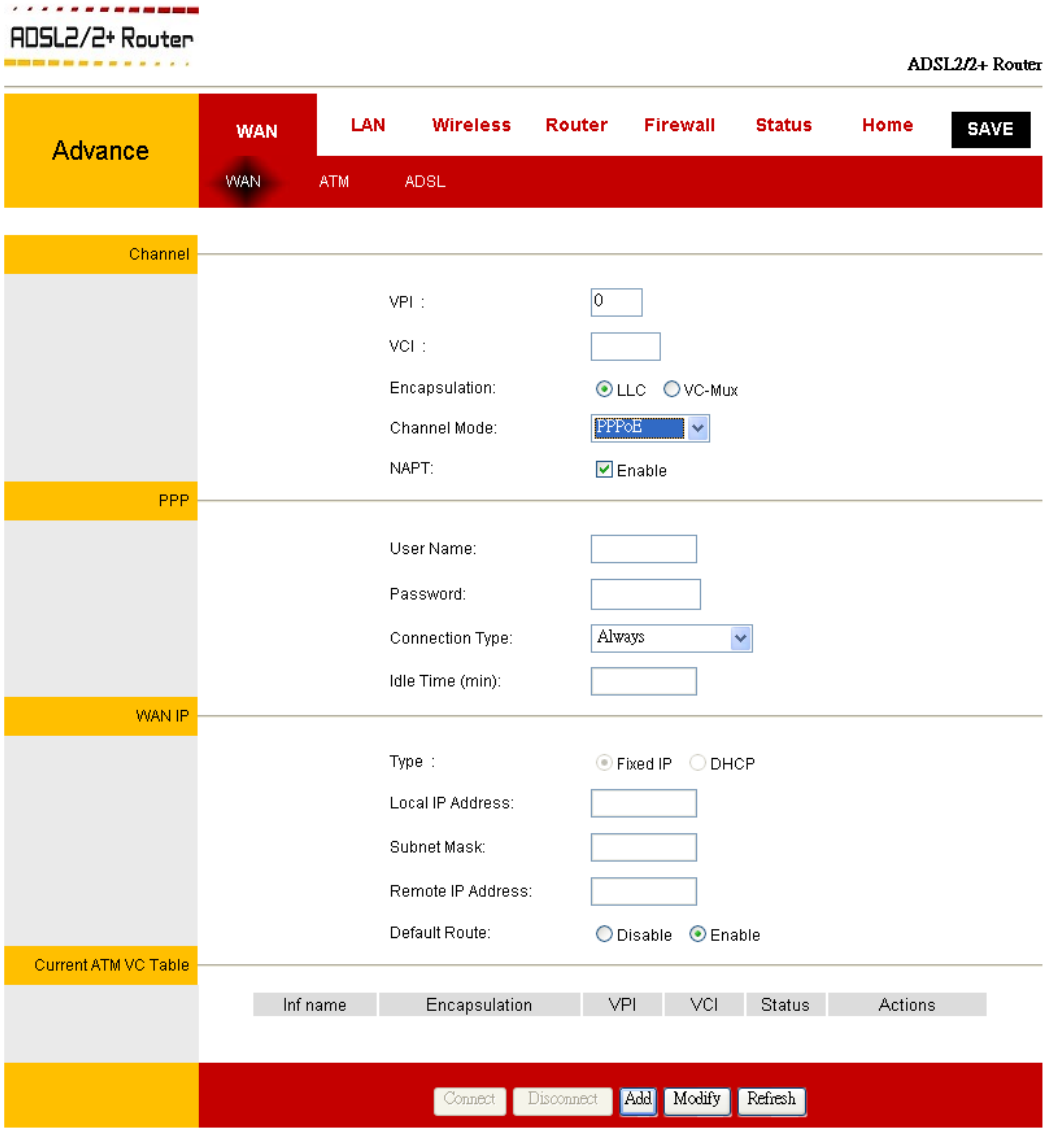
- PPPoE
- PPPoA
- 1483 Bridged
- 1483 MER
- 1483 Routed

The **WAN** setup configuration page enable the user to create, save, delete and select connection profiles as required. (In many cases, only one connection profile will be required and only one connection profile will be used at one time).

4.4.1.2 Creating WAN Connection – PPPoE

PPPoE: When **PPPoE Mode** is selected from the **Channel Mode** drop down manual, the following screen display. Point-to-Point Protocol (PPP) is a method of establishing a network connection between network hosts. PPPoE, also known as RFC 2516, adapts PPP to work over Ethernet for ADSL connections. PPPoE provides a mechanism for authenticating users by providing User Name and Password fields and it is a connection type provided by many ISP or Telecom.

LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.



Refer to next page on the description of the PPPoE options.

■ Channel:

☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an 8-bit field in the ATM cell header. The VPI field specifies this 8-bit identifier for routing.

☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16-bit numerical tag that determines the destination.

☑ **Encapsulation:** There are 2 Encapsulation type:

- ◆ LLC
- ◆ VC-Mux

Note: LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

☑ **Channel Mode:** Select **"PPPoE"** from the drop down manual.

☑ **Enable NAPT:** Select **"Disable"** or **"Enable"** the NAPT functionality. Default setting is **"Enable"**.

■ PPP:

☑ **User Name:** Manually enter your PPPoE User Name which will be provided by your ADSL service provider or ISP.

☑ **Password:** Manually enter your PPPoE Password which will be provided by your ADSL service provider or ISP.

☑ **Connection Type:** Select your connection type from the drop down manual. This 4 Ports 11g Wireless ADSL2/2+ Router provides 3 connection type:

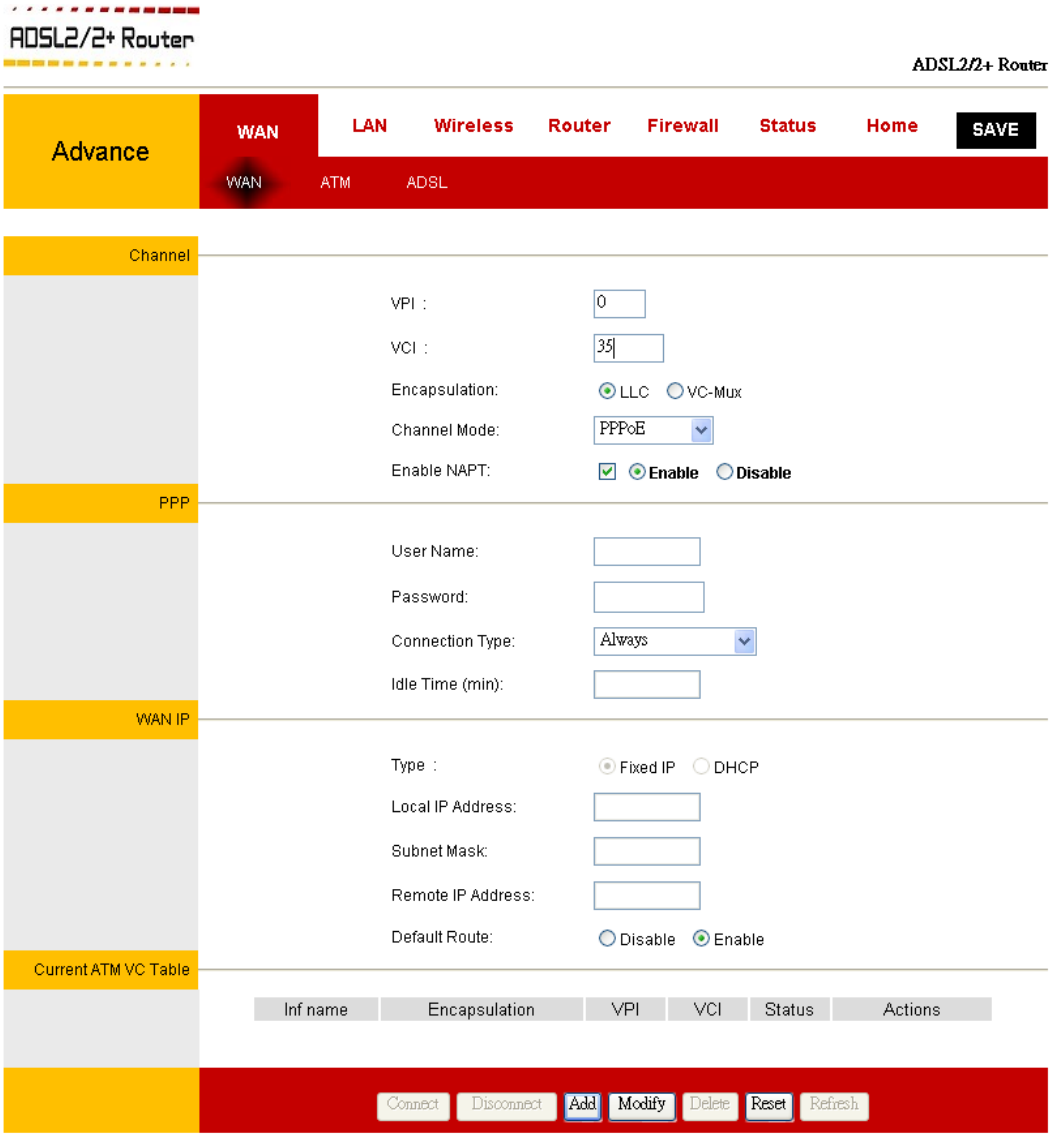
- ◆ Always (Default Setting)
- ◆ Connect on Demand
- ◆ Manual

■ WAN IP:

☑ **Default Route:** Click the radio button to **"Enable"** or **"Disable"** the default Route functionality. Default setting is **Enable**.

4.4.1.2.1 PPPoE Configuration Procedures

1. From the **Advance – WAN – WAN** main page, click and select **PPPoE** connection mode from the Channel Mode drop down manual. The default **PPPoE** connection setup is displayed.



2. Under the **Channel** mode, enter the values of **VPI** and **VCI** settings.

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using 0,35.

3. Click the radio button and elect the Encapsulation type (LLC or VC-Mux).

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using LLC.

4. Check the radio button to **"Enable"** or **"Disable"** the NAPT setting. Leave as it's default setting if your ADSL provider or ISP didn't provide any setting information.

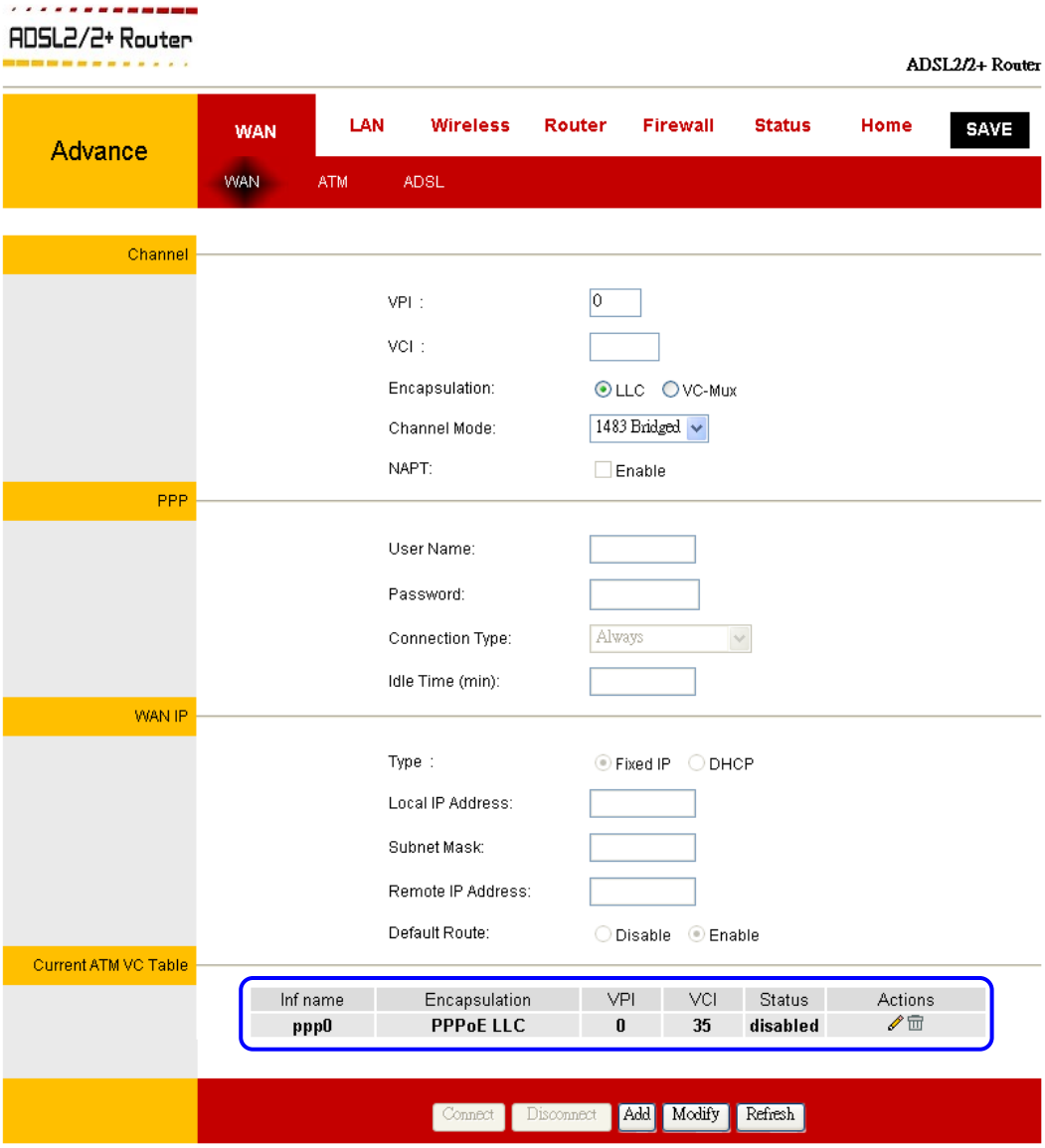
Note: **NAPT:** Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

5. Enter your **Username** and **Password** which will be provided by your ADSL provider or ISP.

6. Select the Connection Type form the drop down manual or leave as it's default setting (Always).

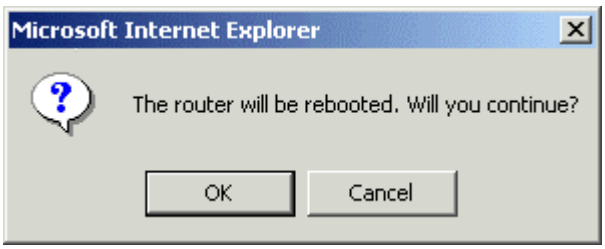
7. Click the radio button to **"Enable"** or **"Disable"** the Default Route functionality or leave as its default (Enable).

8. Click **"Add"** button after setup. The following screen display:

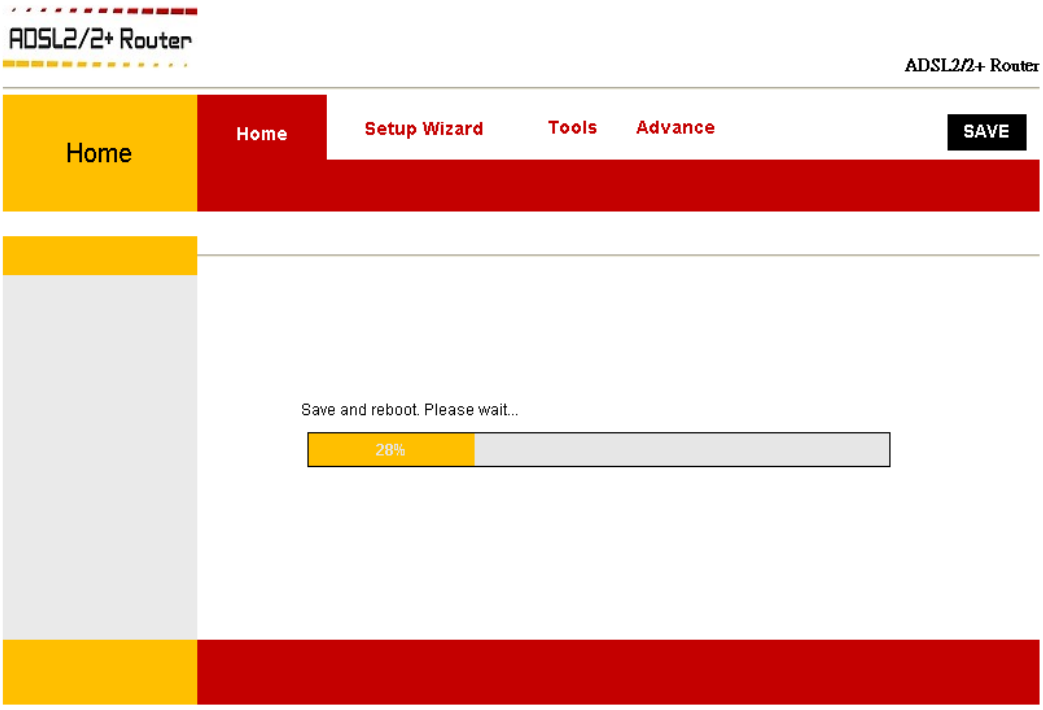


9. You can **"Edit"** ( ) or **"Delete"** ( ) the existing connection profile under the **Actions** column.

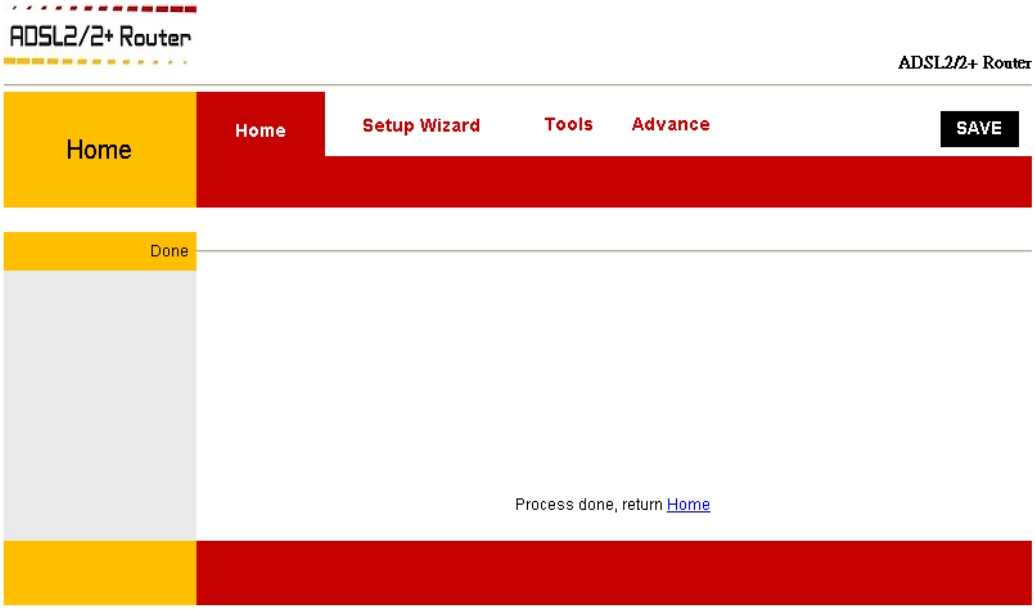
10. To make the change permanent, click on **SAVE**. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



11. The following window display indicates the save setting process.



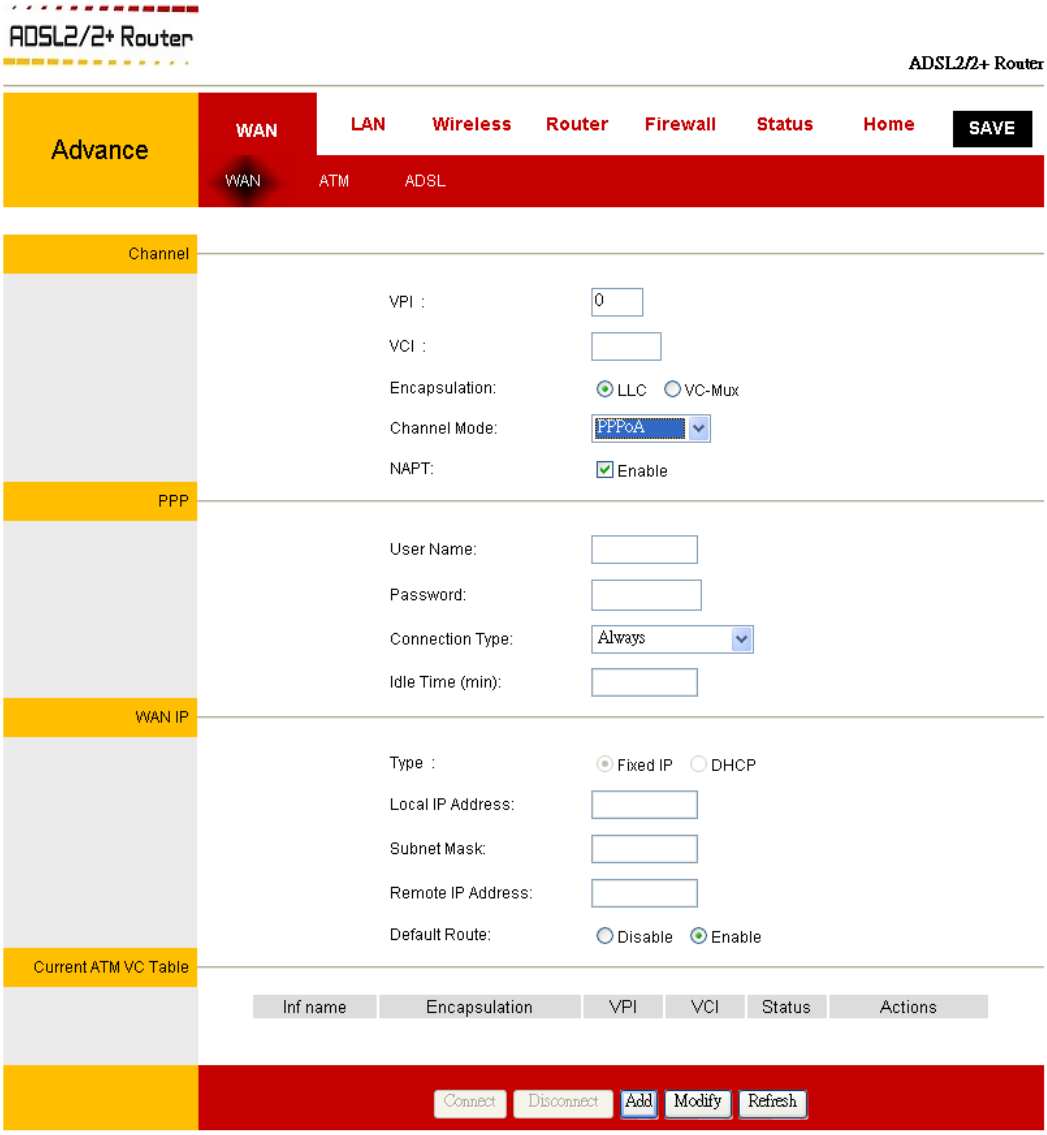
12. The following screen display after the save setting process. Click **Home** to get back to the System Home page. The System Home page will shows all the connection status and system information.



4.4.1.3 Creating WAN Connection – PPPoA

PPPoA: When **PPPoA** mode is selected, the following screen will pop-up. PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets over ATM cells which are carried over the ADSL line. PPP or Point-to-Point protocol is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users.

LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.



■ Channel:

- ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an 8-bit field in the ATM cell header. The VPI field specifies this 8-bit identifier for routing.
- ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16-bit numerical tag that determines the destination.
- ☑ **Encapsulation:** There are 2 Encapsulation type:
  - ◆ LLC
  - ◆ VC-Mux

  Note: LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

- ☑ **Channel Mode:** Select **"PPPoA"** from the drop down manual.

- ☑ **Enable NAPT:** Select **"Disable"** or **"Enable"** the NAPT functionality. Default setting is **"Enable"**.

■ PPP:

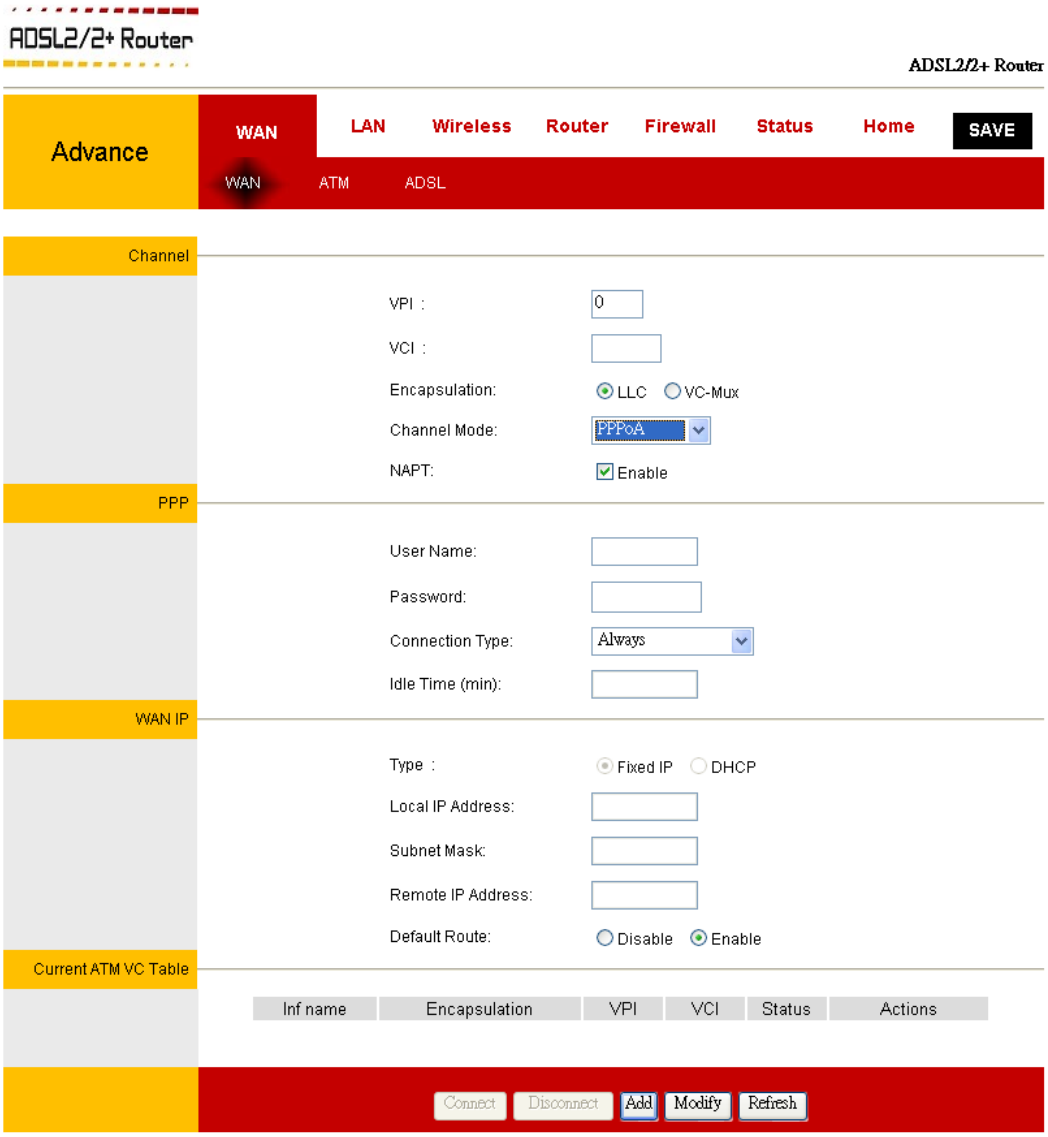
- ☑ **User Name:** Manually enter your PPPoA User Name which will be provided by your ADSL service provider or ISP.
- ☑ **Password:** Manually enter your PPPoA Password which will be provided by your ADSL service provider or ISP.
- ☑ **Connection Type:** Select your connection type from the drop down manual. This 4 Ports 11g Wireless ADSL2/2+ Router provides 3 connection type:
  - ◆ Always (Default Setting)
  - ◆ Connect on Demand
  - ◆ Manual

■ WAN IP:

- ☑ **Default Route:** Click the radio button to **"Enable"** or **"Disable"** the default Route functionality.

4.4.1.3.1 PPPoA Configuration Procedures

1. From the **Advance – WAN – WAN** main page, click and select PPPoA connection mode from the Channel Mode drop down manual. The default PPPoA connection setup is displayed.



2. Under the **Channel** mode, enter the values of **VPI** and **VCI** settings.

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using 0,35.

3. Click the radio button and elect the Encapsulation type (LLC or VC-Mux).

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using LLC.

4. Check the radio button to **"Enable"** or **"Disable"** the NAPT setting. Leave as it's default setting if your ADSL provider or ISP didn't provide any setting information.

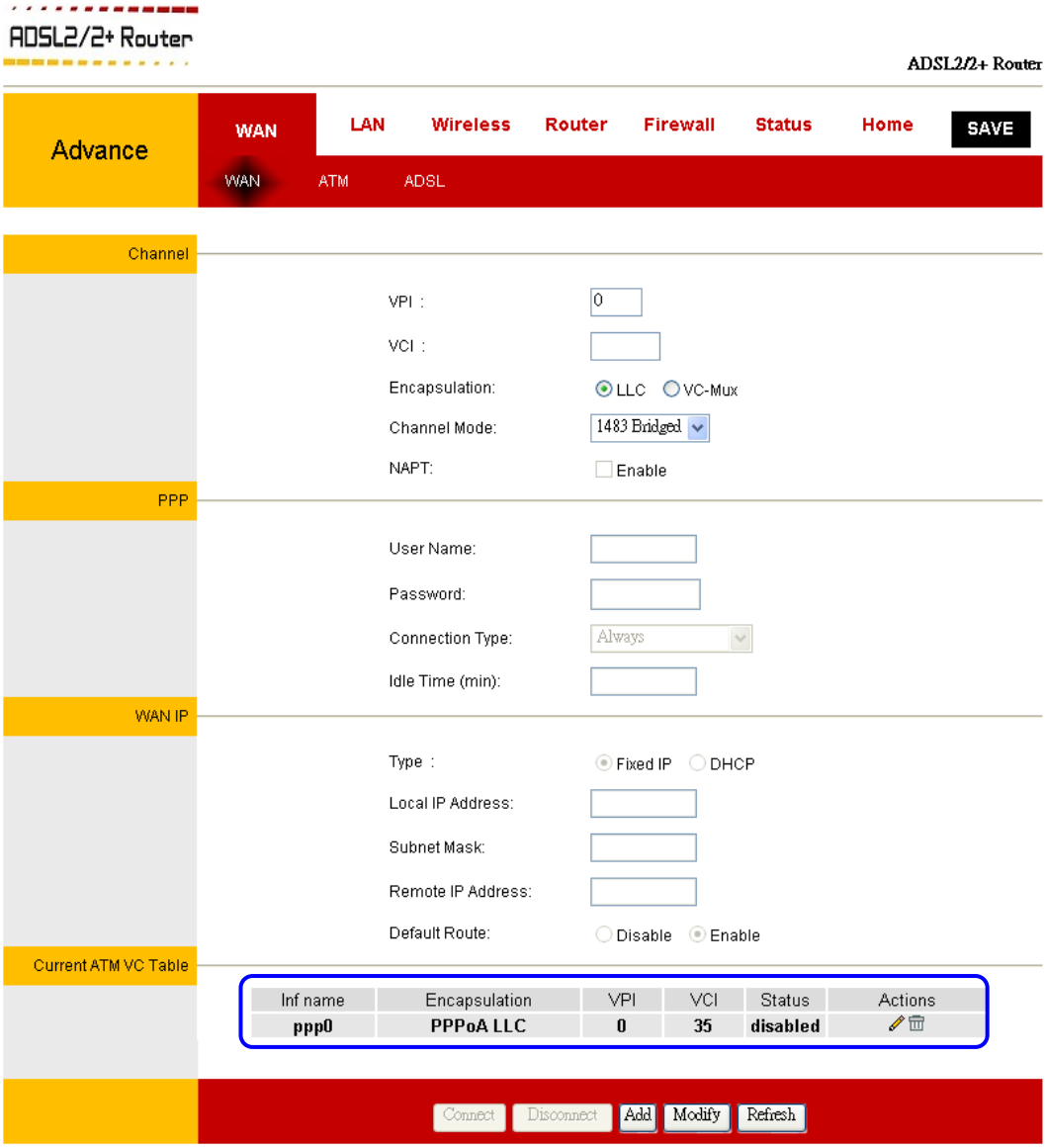
Note: **NAPT:** Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

5. Enter your **Username** and **Password** which will be provided by your ADSL provider or ISP.

6. Select the Connection Type form the drop down manual or leave as it's default setting (Always).

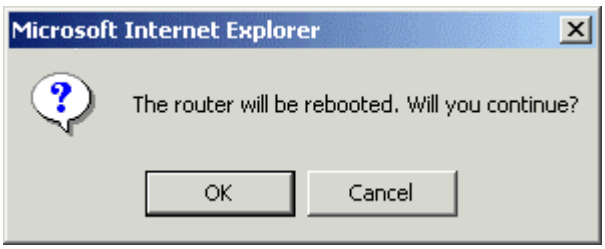
7. Click the radio button to **"Enable"** or **"Disable"** the Default Route functionality or leave as its default (Enable).

8. Click **"Add"** button after setup. The following screen display:

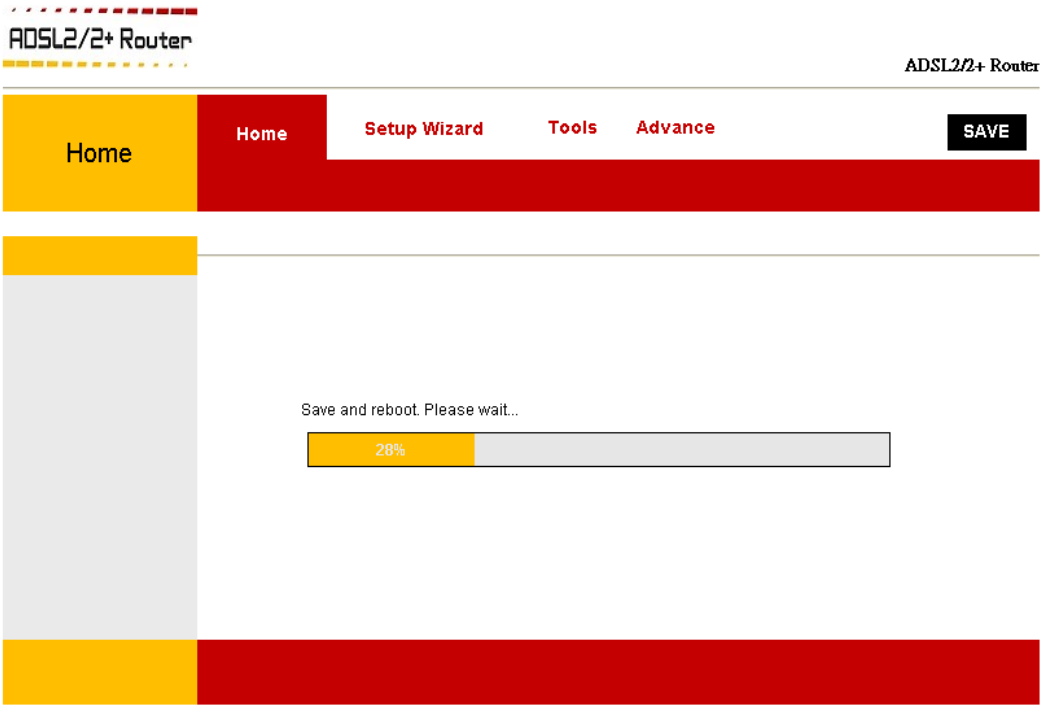


9. You can **"Edit"** ( ) or **"Delete"** ( ) the existing connection profile under the **Actions** column.

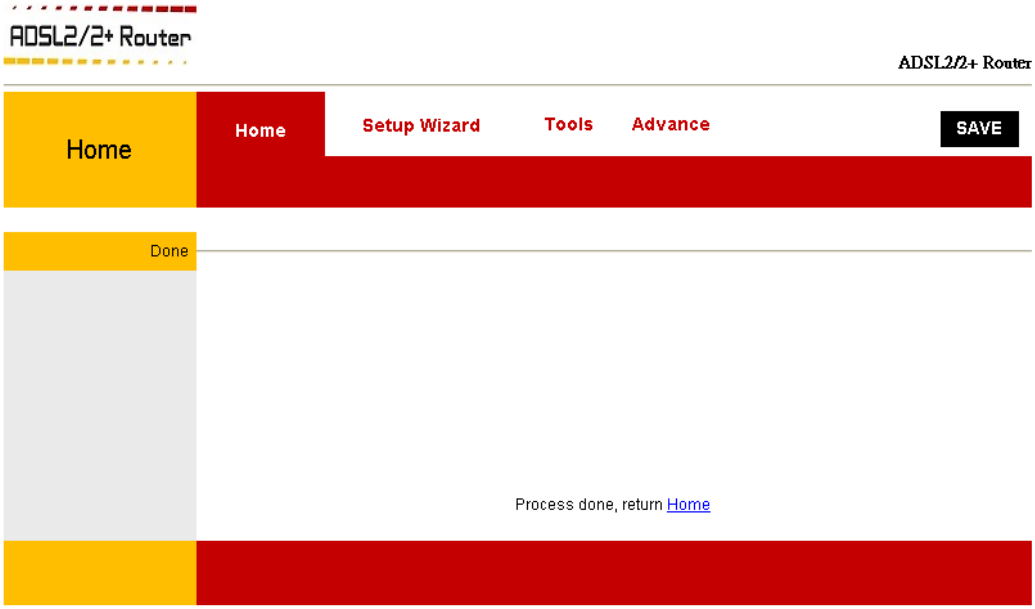
10. To make the change permanent, click on **SAVE**. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



11. The following window display indicates the save setting process.



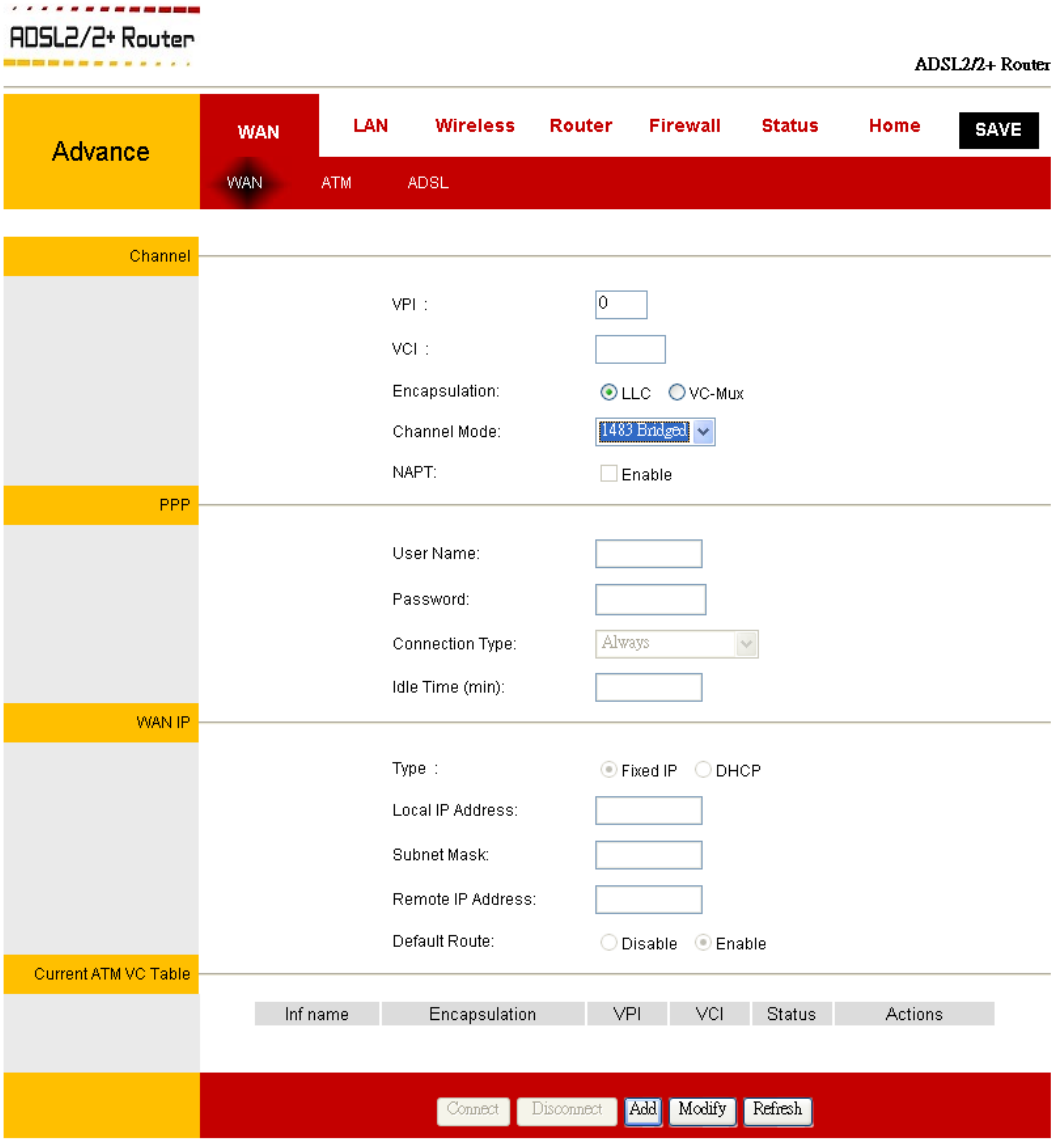
12. The following screen display after the save setting process. Click **Home** to get back to the System Home page. The System Home page will shows all the connection status and system information.



4.4.1.4 Creating WAN Connection – 1483 Bridged

1483 Bridged: When 1483 Bridged mode is selected, the following screen will pop-up. A Bridged connection basically disables the routing, firewall and NAT features of the 4 Ports 11g Wireless ADSL2/2+ Router. In a 1483 Bridged connection, the 4 Ports 11g Wireless ADSL2/2+ Router acts as a modem or hub, and just transmits packets between the WAN interface and the LAN interface. A 1483 Bridged connection assumes that another device is providing the routing functionality that is now disabled in the 4 Ports 11g Wireless ADSL2/2+ Router.

LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.



■ Channel:

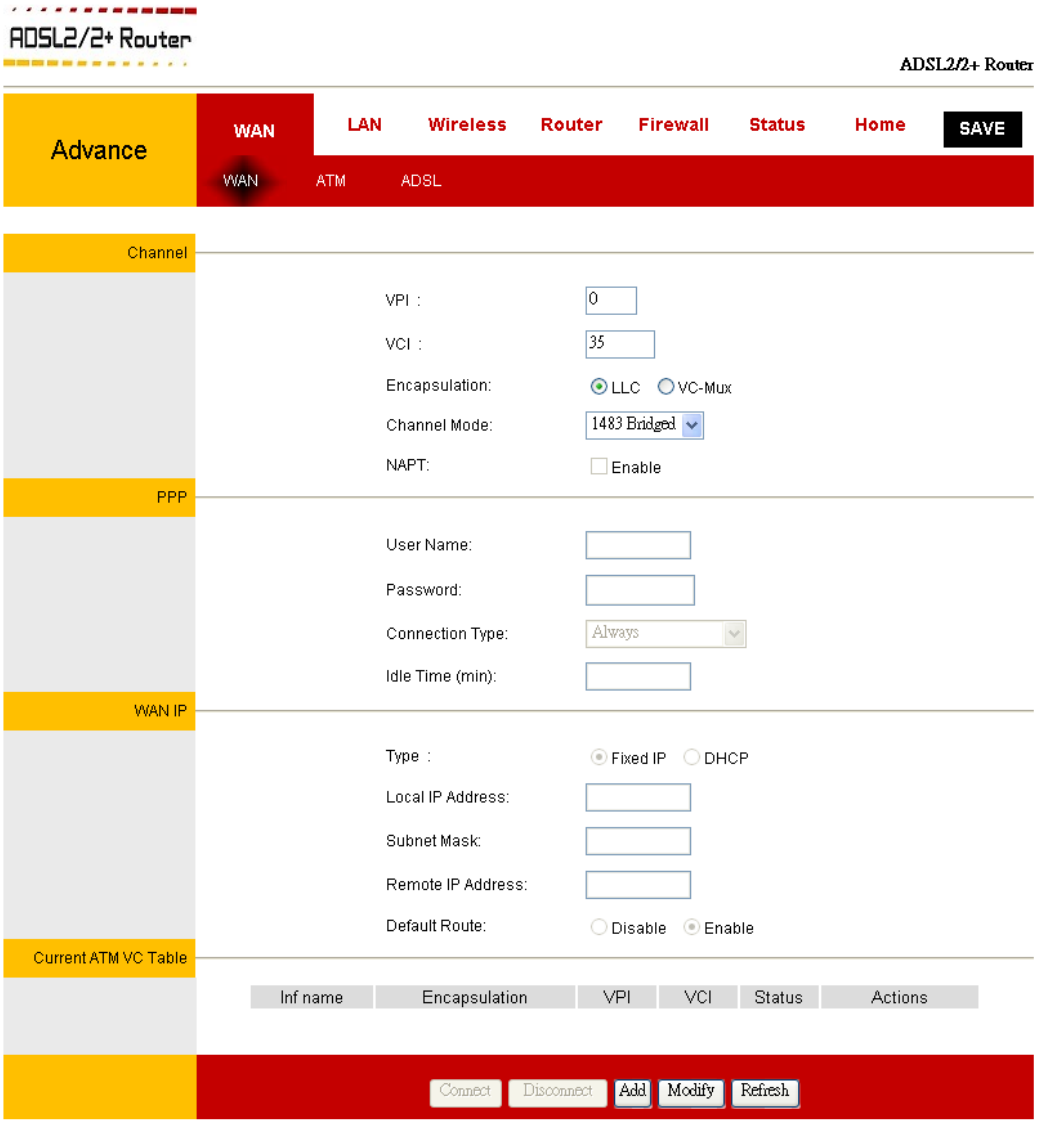
- ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an 8-bit field in the ATM cell header. The VPI field specifies this 8-bit identifier for routing.
- ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16-bit numerical tag that determines the destination.
- ☑ **Encapsulation:** There are 2 Encapsulation type:
  - ◆ LLC
  - ◆ VC-Mux

  Note: LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

- ☑ **Channel Mode:** Select **"1483 Bridged"** from the drop down manual.

4.4.1.4.1 1483 Bridged Configuration Procedures

1. From the **Advance – WAN – WAN** main page, click and select 1483 Bridged connection mode from the Channel Mode drop down manual. The default 1483 Bridged connection setup is displayed.



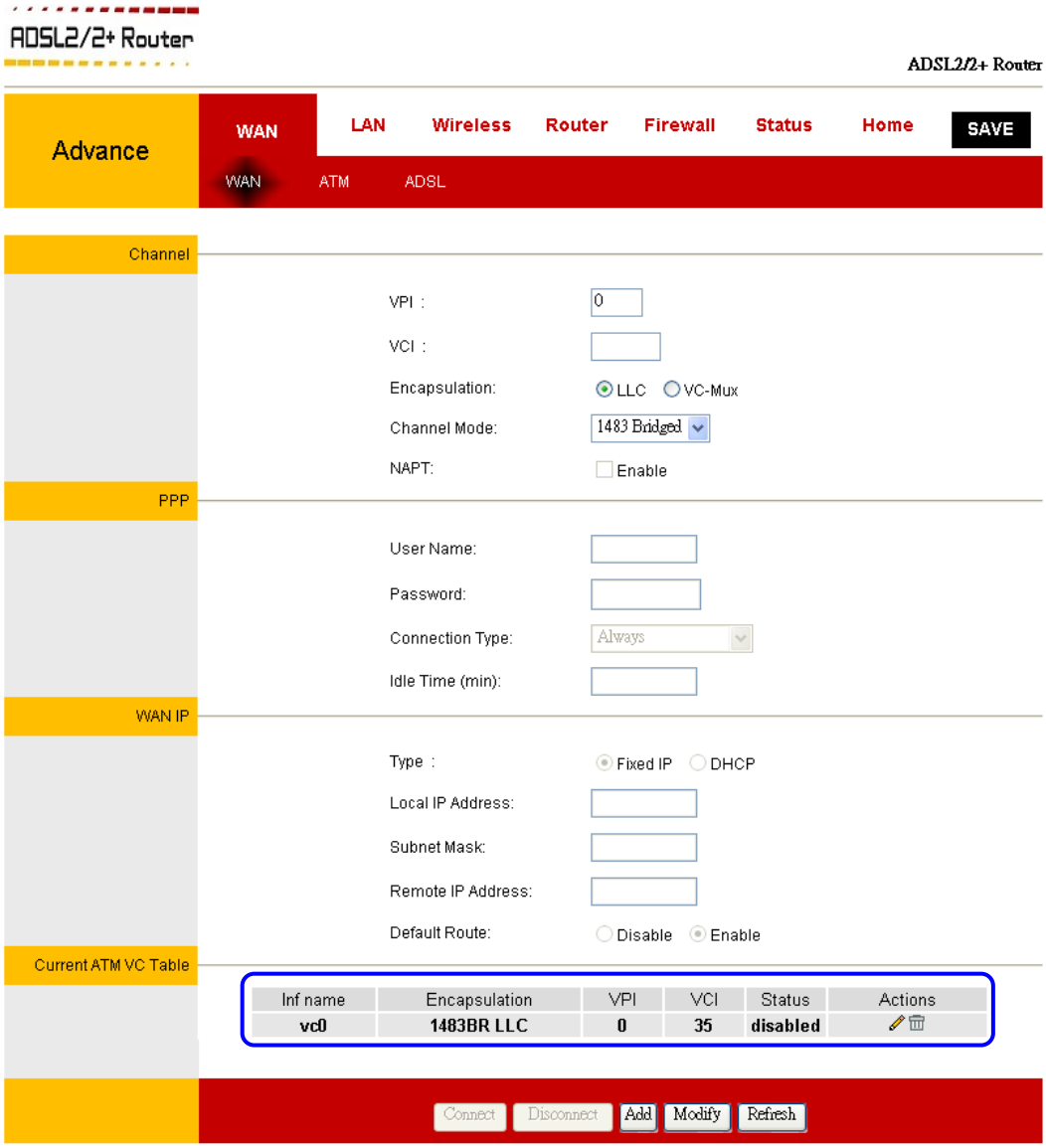
2. Under the **Channel** mode, enter the values of **VPI** and **VCI** settings.

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using 0,35.

3. Click the radio button and elect the Encapsulation type (LLC or VC-Mux).

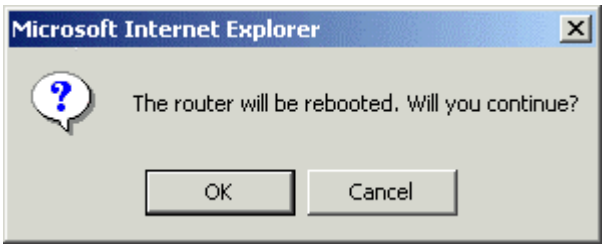
   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using LLC.

4. Click **"Add"** button after setup. The following screen display:

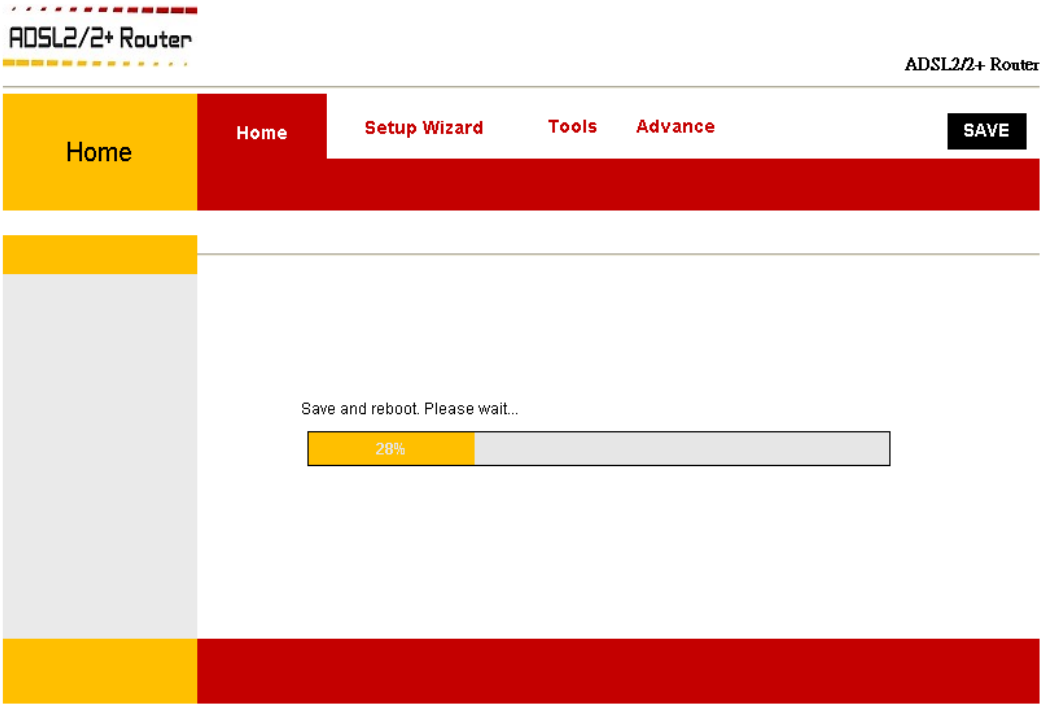


5. You can **"Edit"** ( ) or **"Delete"** ( ) the existing connection profile under the **Actions** column.

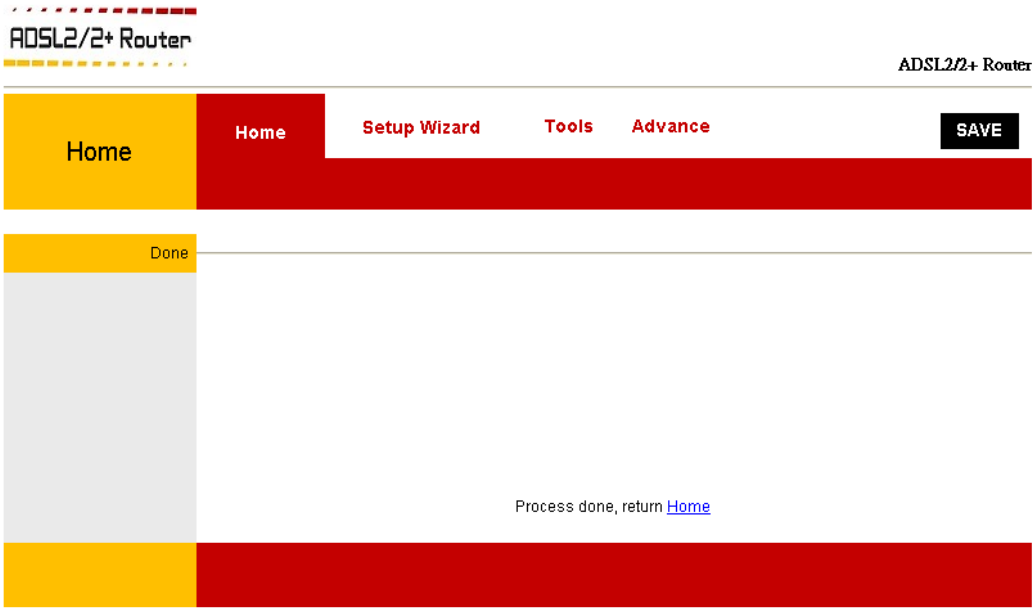
6. To make the change permanent, click on **SAVE**. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



7. The following window display indicates the save setting process.

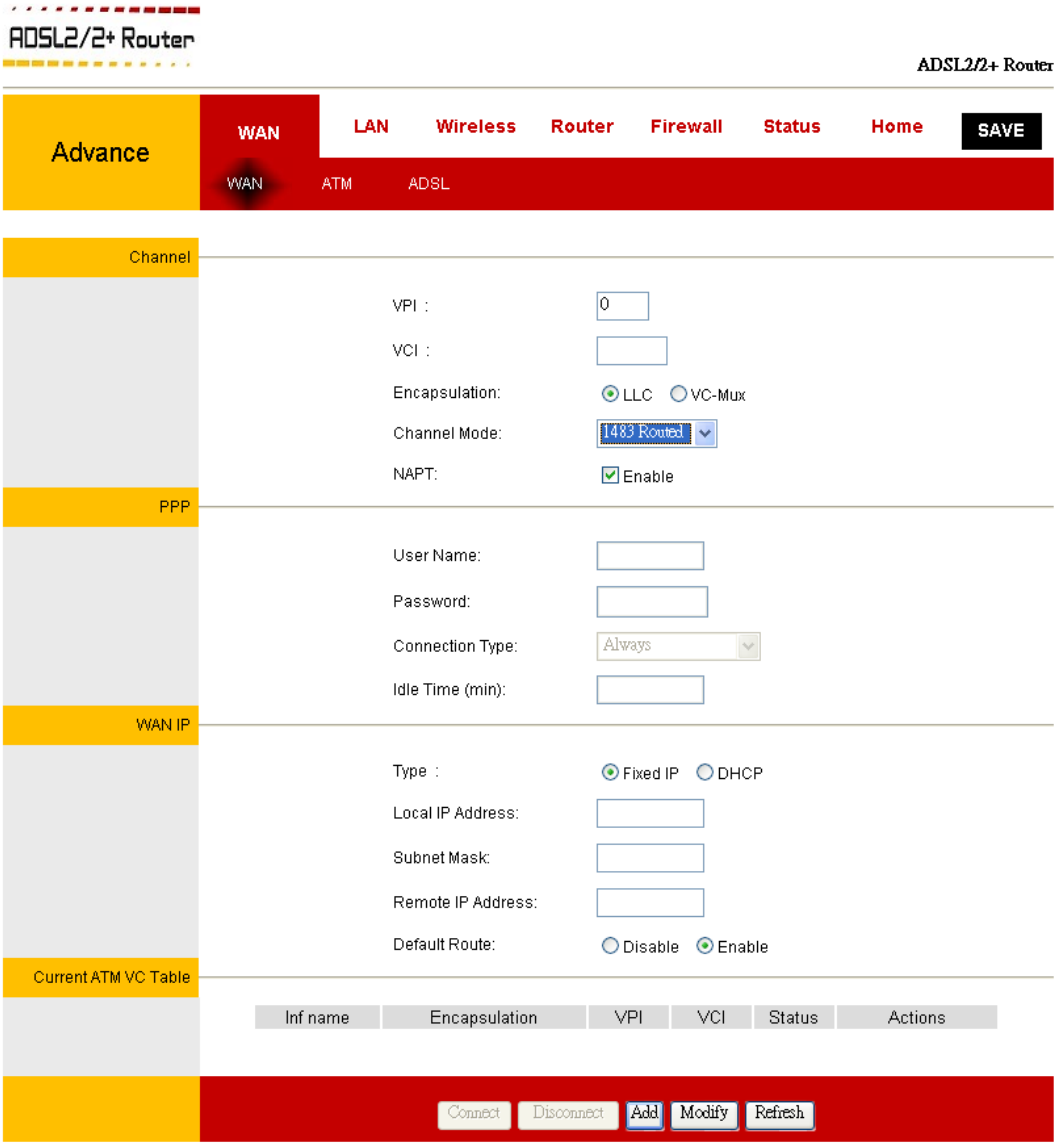


8. The following screen display after the save setting process. Click **Home** to get back to the System Home page. The System Home page will shows all the connection status and system information.



4.4.1.5 Creating WAN Connection – 1483 Routed

1483 Routed: When **1483 Routed** mode is selected, the following screen will pop-up. Most Internet users are provided with a dynamic IP address by their ISP for each session, however certain situations call for a **Fixed** (Or **Static**) IP address. Fixed (Or Static) is used whenever a known Fixed (Or Static) IP is assigned. The accompanying information such as the **Subnet mask**, **Local IP Address** and the **Remote IP Address** should also be specified. Up to three Domain Name Server (**DNS**) addresses can also be specified (Click **Advance – Router – DNS** configuration page and fill in the DNS provided by your ISP). These servers would enable you to have access to other web servers. Valid IP addresses range is from 0.0.0.0 to 255.255.255.255.



■ Channel:

☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an 8-bit field in the ATM cell header. The VPI field specifies this 8-bit identifier for routing.

☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16-bit numerical tag that determines the destination.

☑ **Encapsulation:** There are 2 Encapsulation type:

- ◆ LLC
- ◆ VC-Mux

Note: LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

☑ **Channel Mode:** Select **"1483 Routed"** from the drop down manual.

☑ **Enable NAPT:** Select **"Disable"** or **"Enable"** the NAPT functionality. Default setting is **"Enable"**.

■ WAN IP:

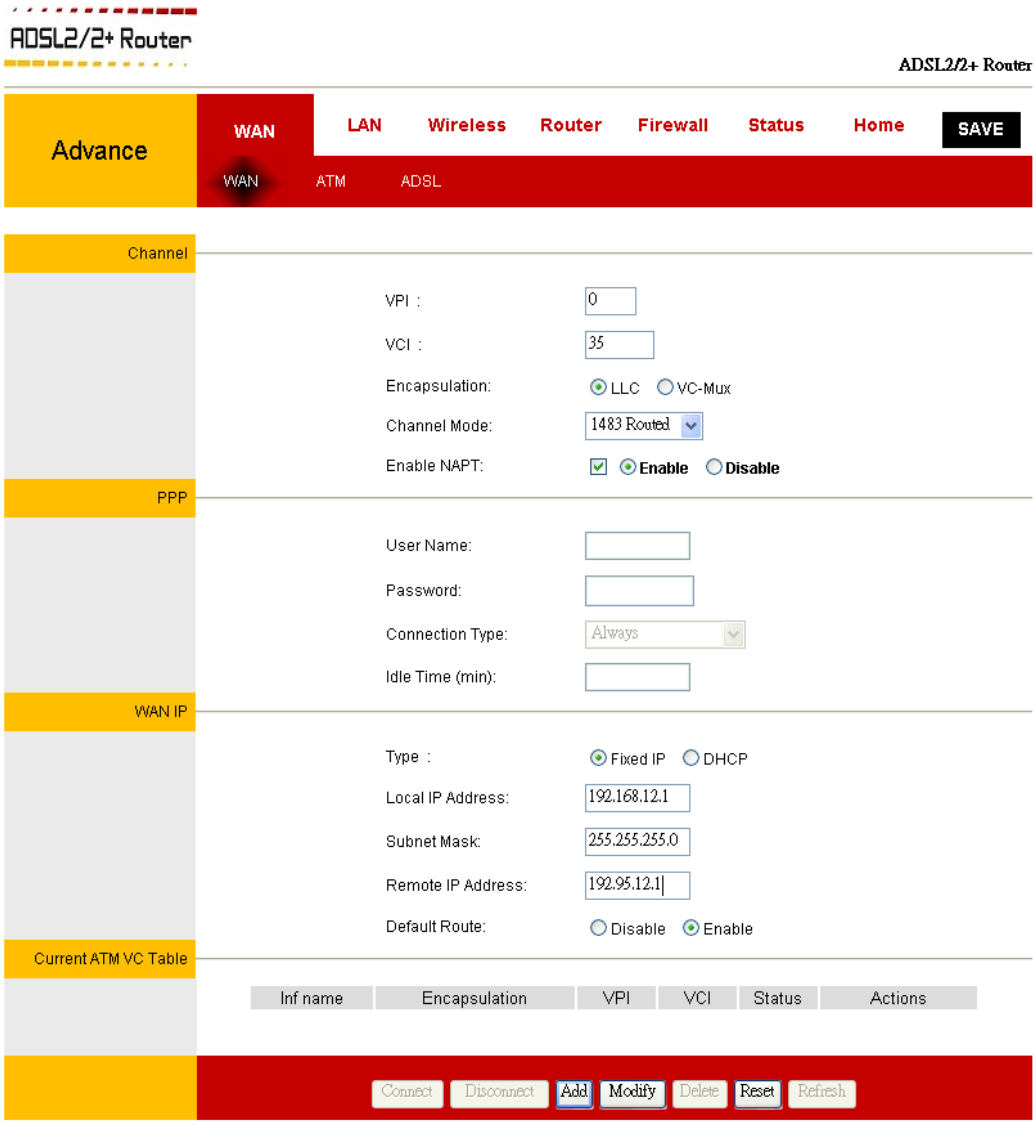
☑ **Type:** Click the radio button to select **"Fixed IP"** or **"DHCP"** mode.

- ◆ **Fixed IP:** You need to fill in the **"Local IP Address"**, **"Subnet Mask"**, **"Remote IP Address"** and **"DNS"** setting which will be provided by your ADSL Service provider or ISP. You need to go to **Advance – Router – DNS** configuration page to fill in your DNS setting.
- ◆ **DHCP:** Dynamic Host Configuration Protocol (DHCP) allows the 4 Ports 11g Wireless ADSL2/2+ Router to automatically obtain the IP address from the server. This option is commonly used in situations where the IP address is dynamically assigned and is not known prior to assignment.

☑ **Default Route:** Click the radio button to **"Enable"** or **"Disable"** the Default Route functionality.

4.4.1.5.1 1483 Routed Configuration Procedures – Fixed IP

1. From the **Advance – WAN – WAN** main page, click and select **1483 Routed** connection mode from the Channel Mode drop down manual. The default 1483 Routed connection setup is displayed.



2. Under the **Channel** mode, enter the values of **VPI** and **VCI** settings.

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using 0,35.

3. Click the radio button and elect the Encapsulation type (LLC or VC-Mux).

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using LLC.

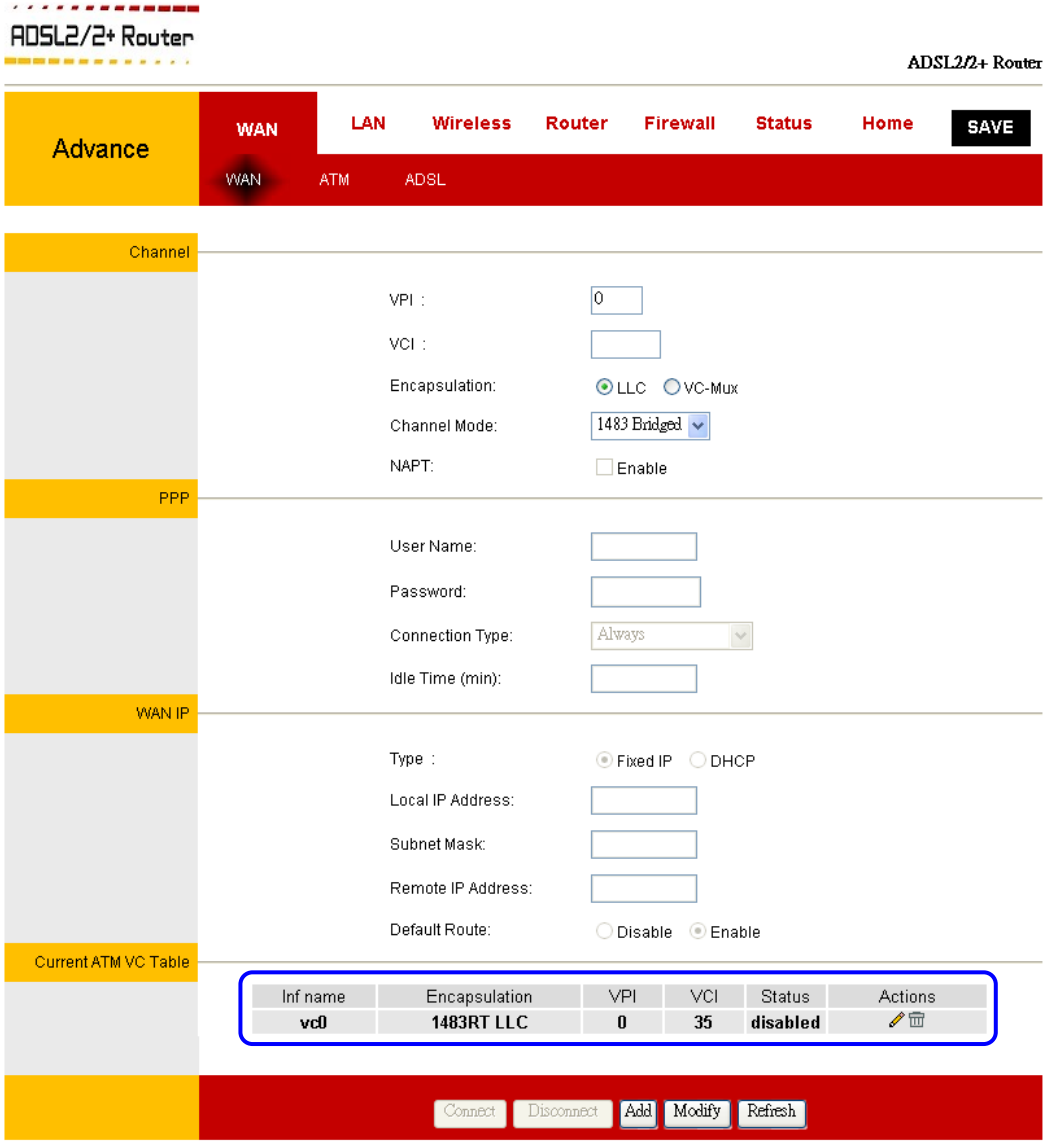
4. Check the radio button to **"Enable"** or **"Disable"** the NAPT setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

   Note: **NAPT:** Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

5. Under the **WAN IP** mode, enter the **"Local IP Address"**, **"Subnet Mask"**, **"Remote IP Address"** and **"DNS"** setting if you are using the **Fixed IP** (Or Static IP) mode. These information/data will be provided by your ADSL Service provider or ISP.

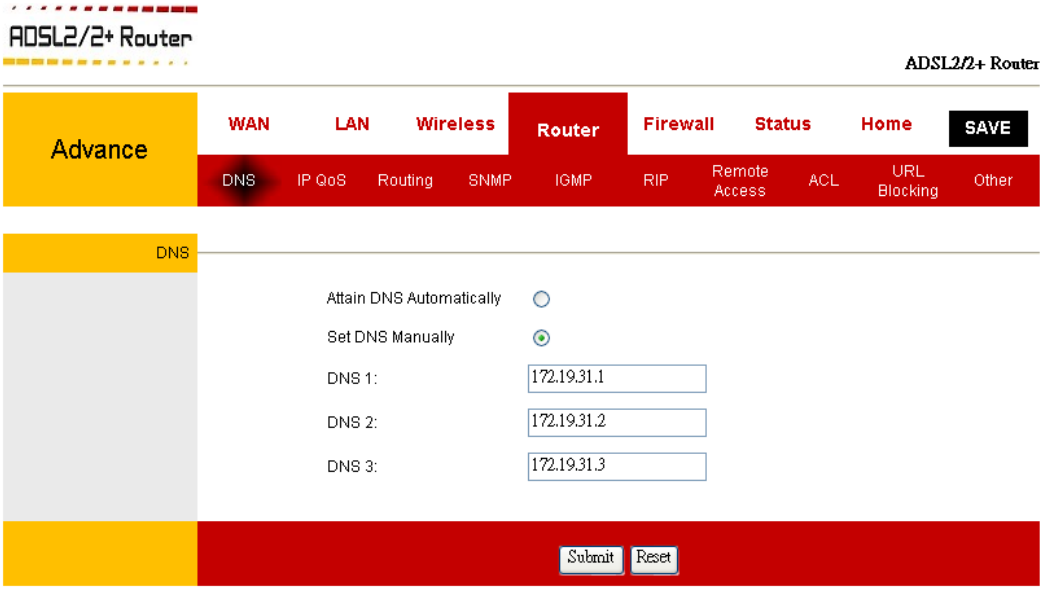
6. Check the radio button to **"Enable"** or **"Disable"** the Default Route setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

7. Click **"Add"** button after setup. The following screen display:



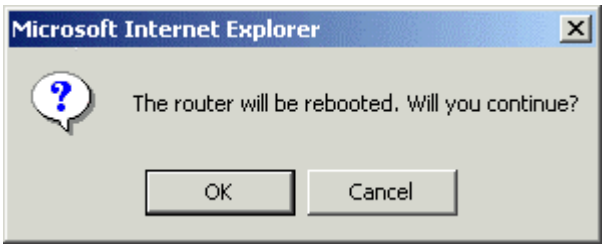
8. You can **"Edit"** ( ) or **"Delete"** ( ) the existing connection profile under the **Actions** column.

9. Click on **Advance – Router – DNS**, the following screen display. Click on **Set DNS Manually** and fill in the DNS setting which will be provided by your ADSL Service provider. Click Submit after setup. A **Change setting successfully** screen display. Click **OK** and return to the DNS setting homepage.

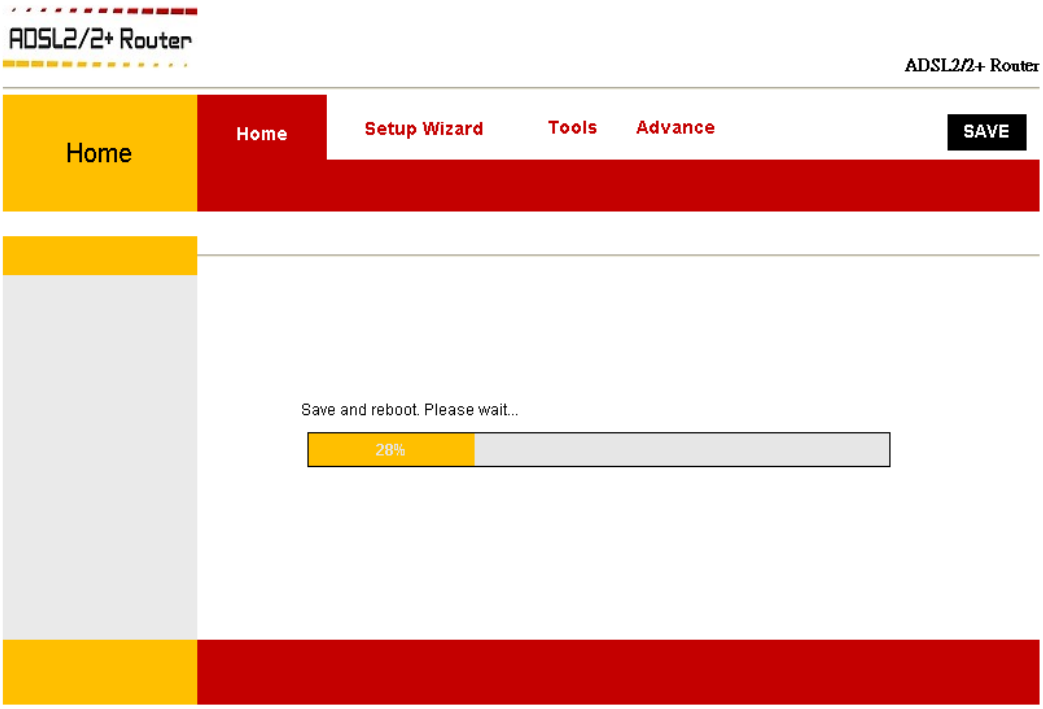


10. Click **Advance – WAN – WAN** tab and return back to the WAN configuration home page.

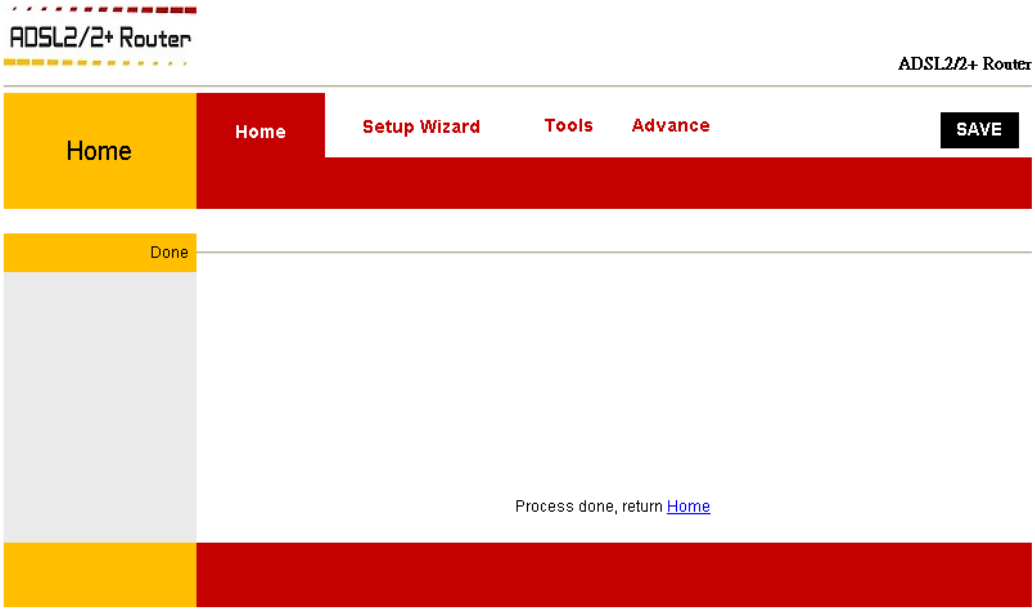
11. To make the change permanent, click on **SAVE**. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



12. The following window display indicates the save setting process.

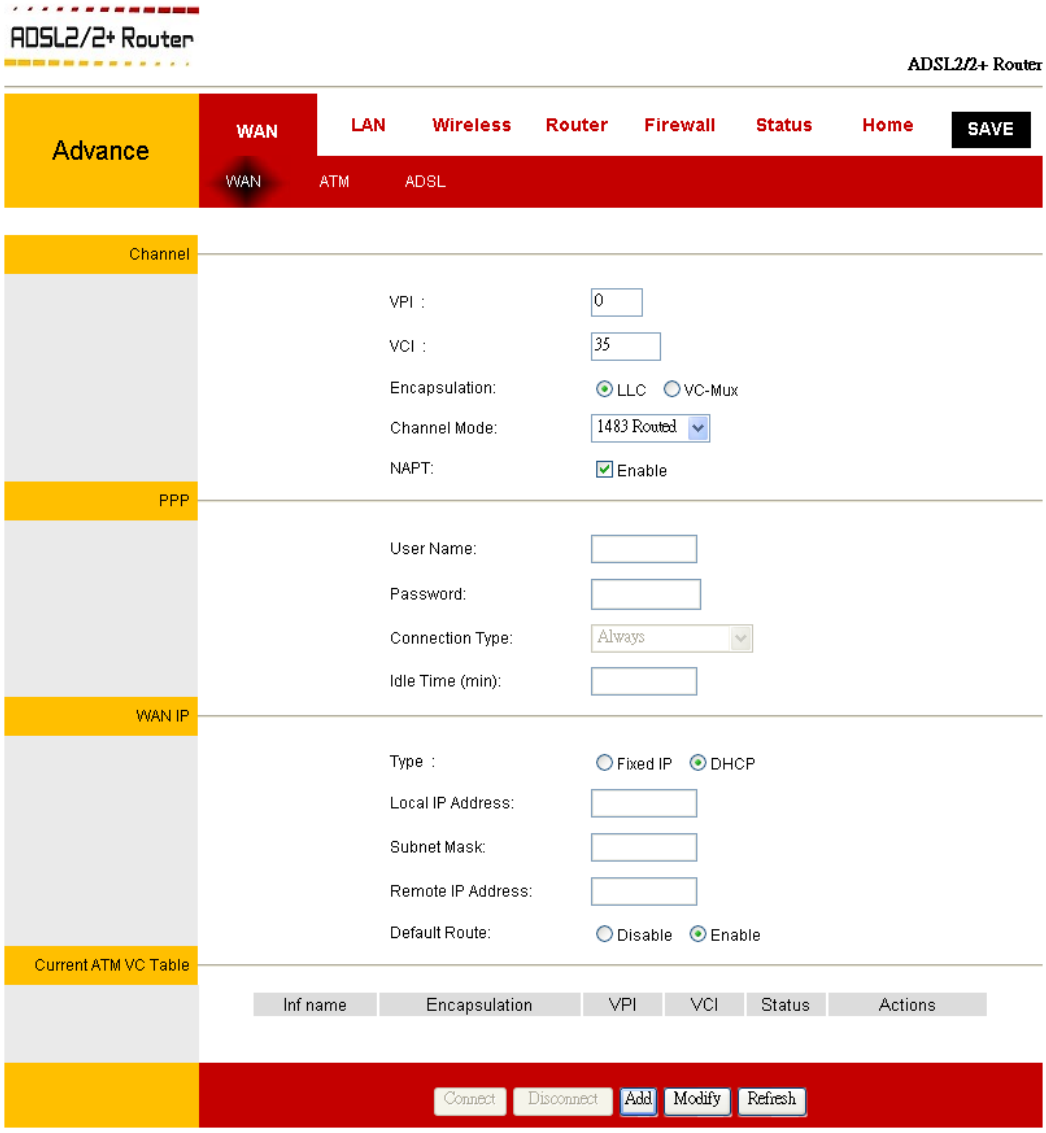


13. The following screen display after the save setting process. Click **Home** to get back to the System Home page. The System Home page will shows all the connection status and system information.



4.4.1.5.2 1483 Routed Configuration Procedures – DHCP

1. From the **Advance – WAN – WAN** main page, click and select **1483 Routed** connection mode from the Channel Mode drop down manual. The default 1483 Routed connection setup is displayed.



2. Under the **Channel** mode, enter the values of **VPI** and **VCI** settings.

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using 0,35.

3. Click the radio button and elect the Encapsulation type (LLC or VC-Mux).

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using LLC.

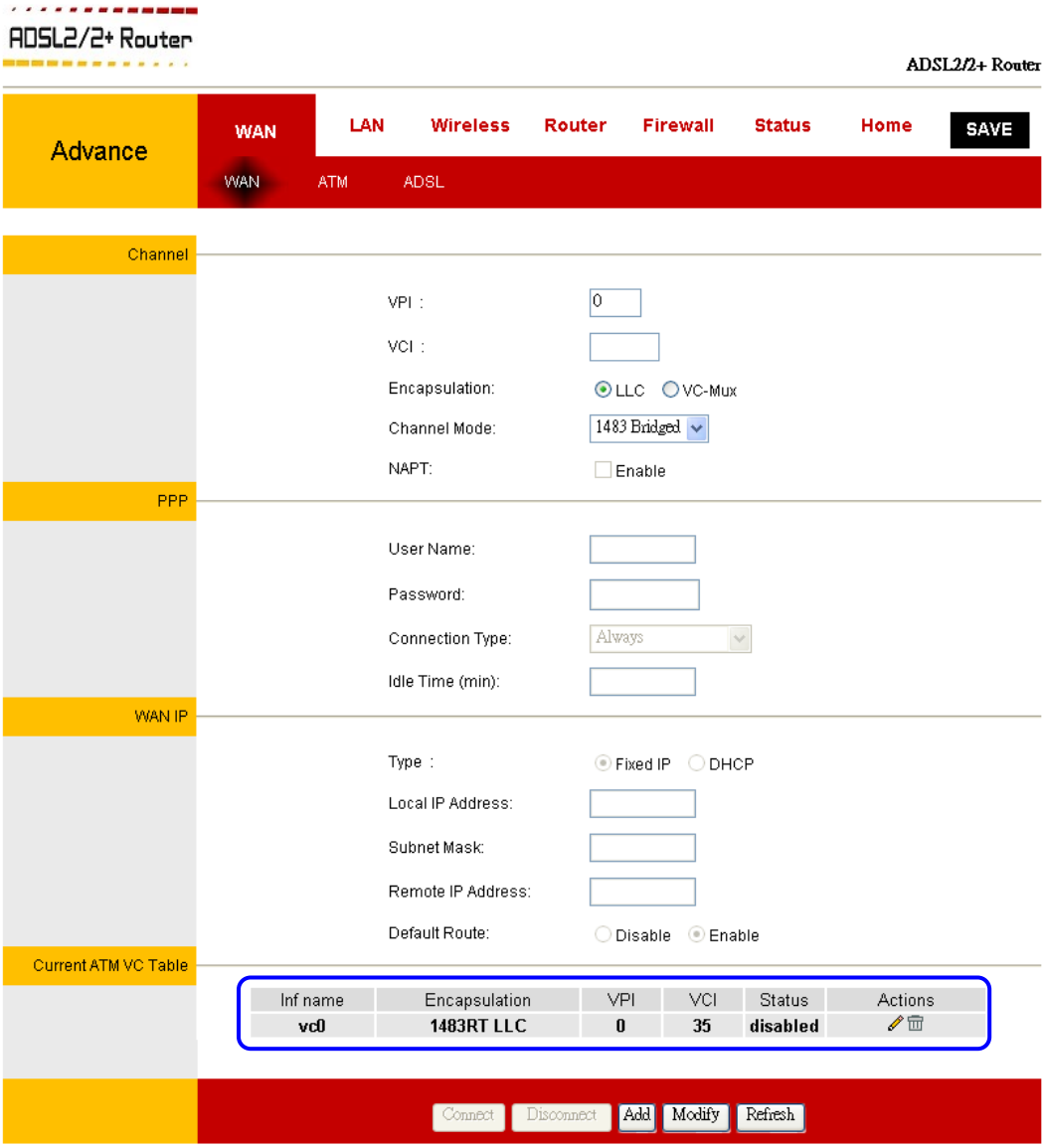
4. Check the radio button to **"Enable"** or **"Disable"** the NAPT setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

Note: **NAPT:** Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

5. Under the **WAN IP** mode, if you select DHCP as your connection type, nothing needed to fill. In this case the ADSL service provider is using Dynamic IP (Or DHCP) mode.

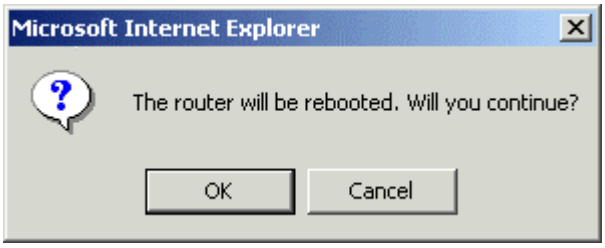
6. Check the radio button to **"Enable"** or **"Disable"** the Default Route setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

7. Click **"Add"** button after setup. The following screen display:

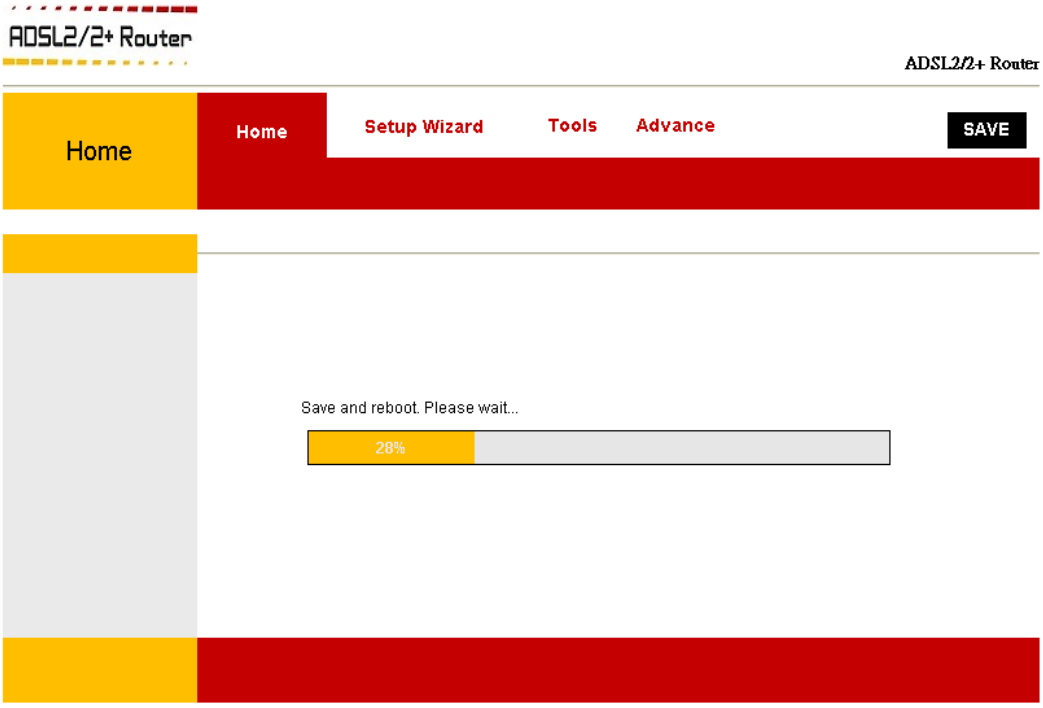


8. You can **"Edit"** ( ) or **"Delete"** ( ) the existing connection profile under the **Actions** column.

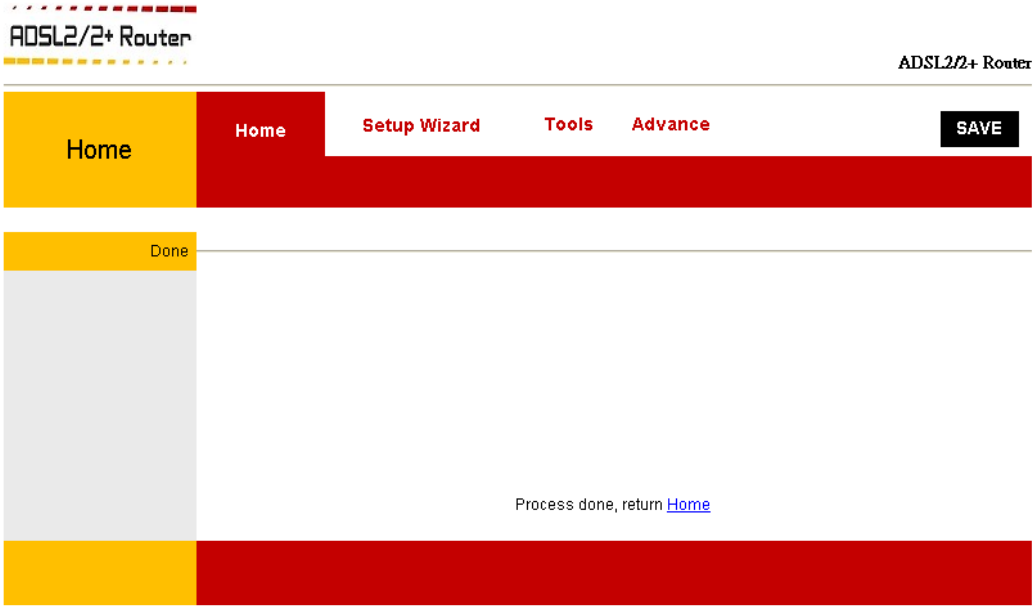
9. To make the change permanent, click on **SAVE**. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



10. The following window display indicates the save setting process.

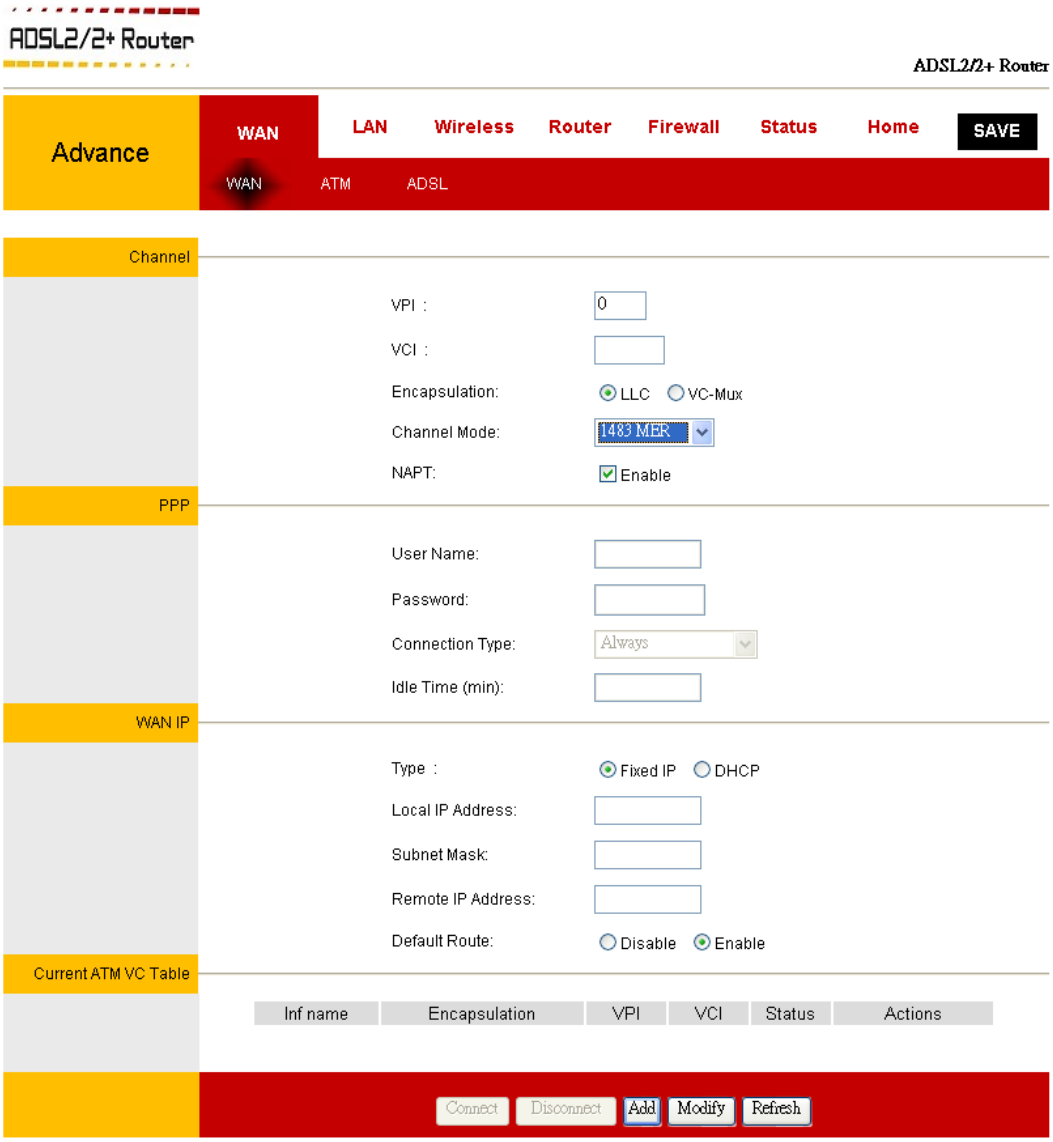


11. The following screen display after the save setting process. Click **Home** to get back to the System Home page. The System Home page will shows all the connection status and system information.



4.4.1.6 Creating WAN Connection – 1483 MER

1483 MER: 1483 MER also commonly known as 1483 Bridged Router mode. When 1483 MER mode is selected, the following screen will pop-up. Most Internet users are provided with a dynamic IP address by their ISP for each session, however certain situations call for a Fixed (Or Static) IP address. Fixed (Or Static) is used whenever a known Fixed (Or Static) IP is assigned. The accompanying information such as the Subnet mask and the gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers would enable you to have access to other web servers. Valid IP addresses range is from 0.0.0.0 to 255.255.255.255.



■ Channel:

☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an 8-bit field in the ATM cell header. The VPI field specifies this 8-bit identifier for routing.

☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16-bit numerical tag that determines the destination.

☑ **Encapsulation:** There are 2 Encapsulation type:

- ◆ LLC
- ◆ VC-Mux

Note: LLC and VC-Mux are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

☑ **Channel Mode:** Select **"1483 Routed"** from the drop down manual.

☑ **Enable NAPT:** Select **"Disable"** or **"Enable"** the NAPT functionality. Default setting is **"Enable"**.

■ WAN IP:

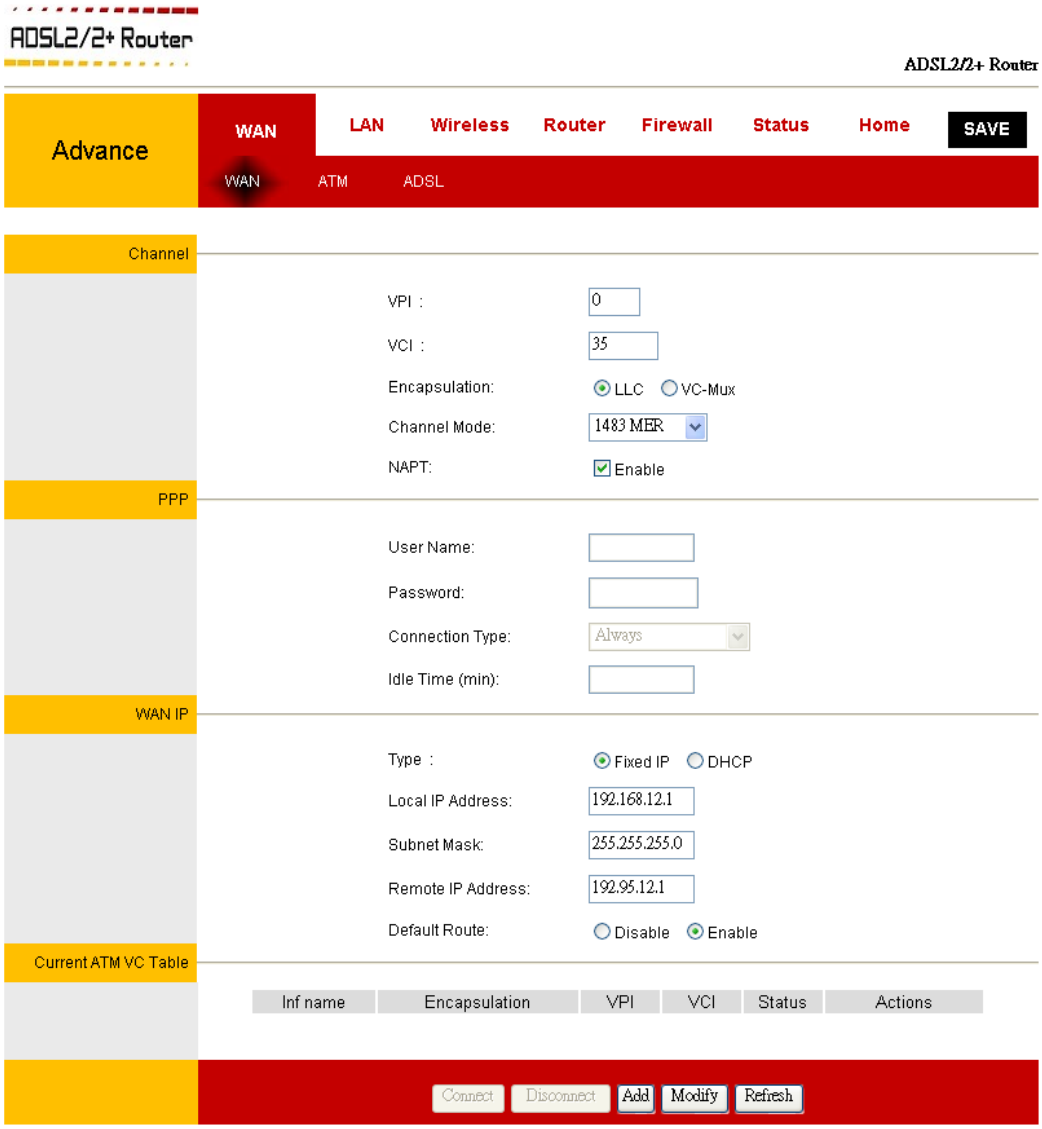
☑ **Type:** Click the radio button to select **"Fixed IP"** or **"DHCP"** mode.

- ◆ **Fixed IP:** You need to fill in the **"Local IP Address"**, **"Subnet Mask"**, **"Remote IP Address"** and **"DNS"** setting which will be provided by your ADSL Service provider or ISP.
- ◆ **DHCP:** Dynamic Host Configuration Protocol (DHCP) allows the 4 Ports 11g Wireless ADSL2/2+ Router to automatically obtain the IP address from the server. This option is commonly used in situations where the IP address is dynamically assigned and is not known prior to assignment.

☑ **Default Route:** Click the radio button to **"Enable"** or **"Disable"** the Default Route functionality.

4.4.1.6.1 1483 MER Configuration Procedures – Fixed IP

1. From the **Advance – WAN – WAN** main page, click and select 1483 MER connection mode from the Channel Mode drop down manual. The default 1483 MER connection setup is displayed.



2. Under the **Channel** mode, enter the values of **VPI** and **VCI** settings.

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using 0,35.

3. Click the radio button and elect the Encapsulation type (LLC or VC-Mux).

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using LLC.

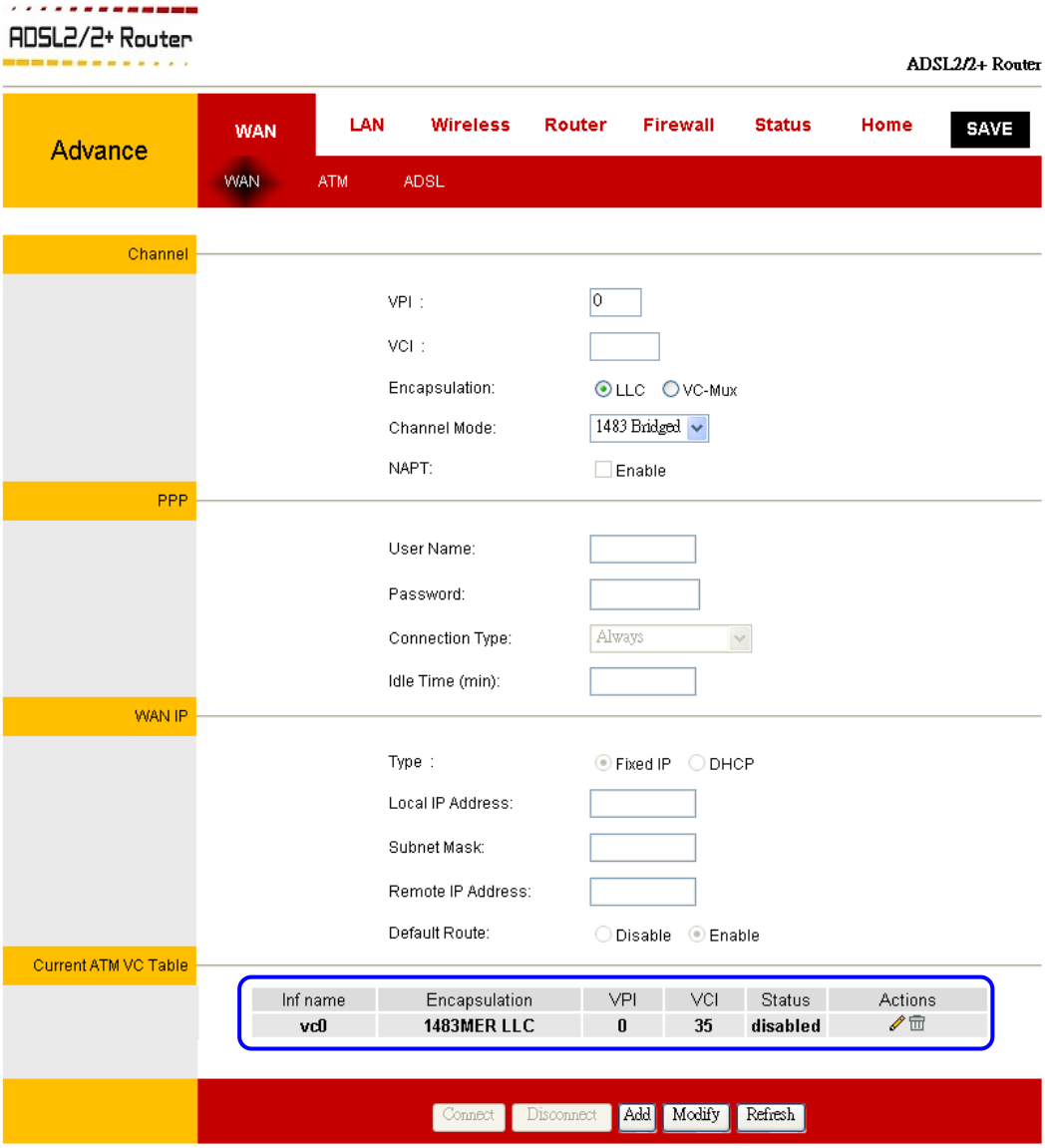
4. Check the radio button to **"Enable"** or **"Disable"** the NAPT setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

   Note: **NAPT:** Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

5. Under the **WAN IP** mode, enter the **"Local IP Address"**, **"Subnet Mask"**, **"Remote IP Address"** and **"DNS"** setting if you are using the **Fixed IP** (Or Static IP) mode. These information/data will be provided by your ADSL Service provider or ISP.

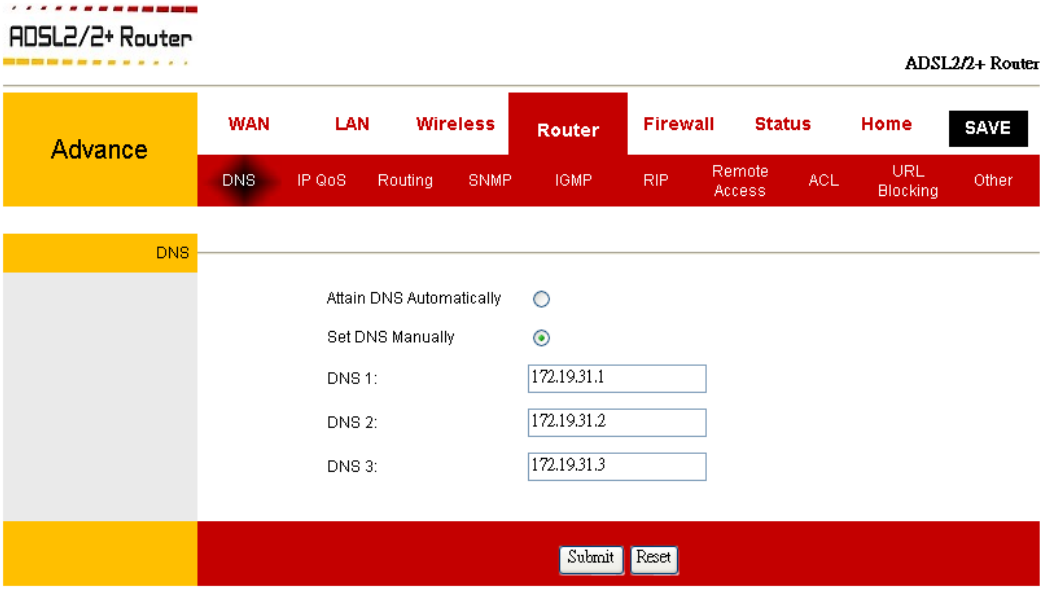
6. Check the radio button to **"Enable"** or **"Disable"** the Default Route setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

7. Click **"Add"** button after setup. The following screen display:



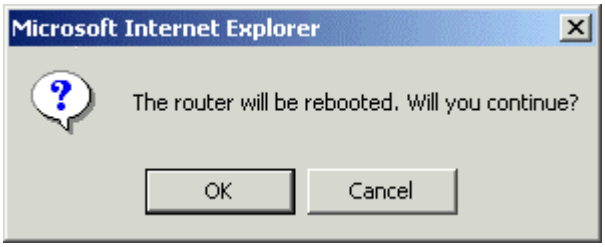
8. You can **"Edit"** ( ) or **"Delete"** ( ) the existing connection profile under the **Actions** column.

9. Click on **Advance – Router – DNS**, the following screen display. Click on **Set DNS Manually** and fill in the DNS setting which will be provided by your ADSL Service provider. Click **Submit** after setup. A **Change setting successfully** screen display. Click **OK** and return to the DNS setting homepage.

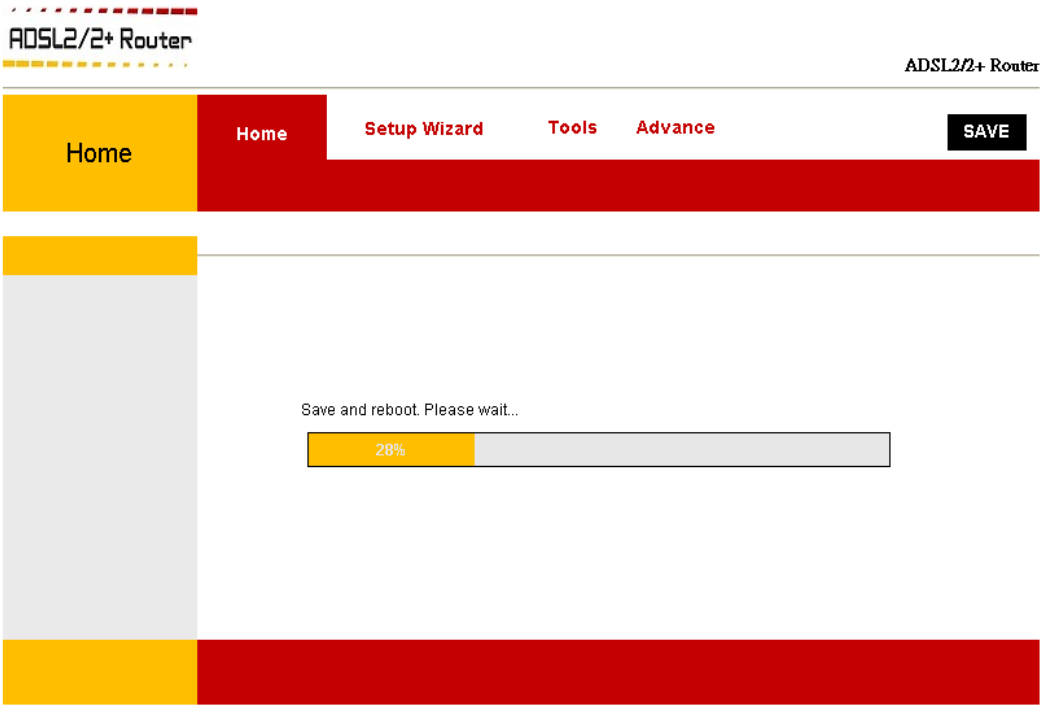


10. Click **Advance – WAN – WAN** tab and return back to the WAN configuration home page.

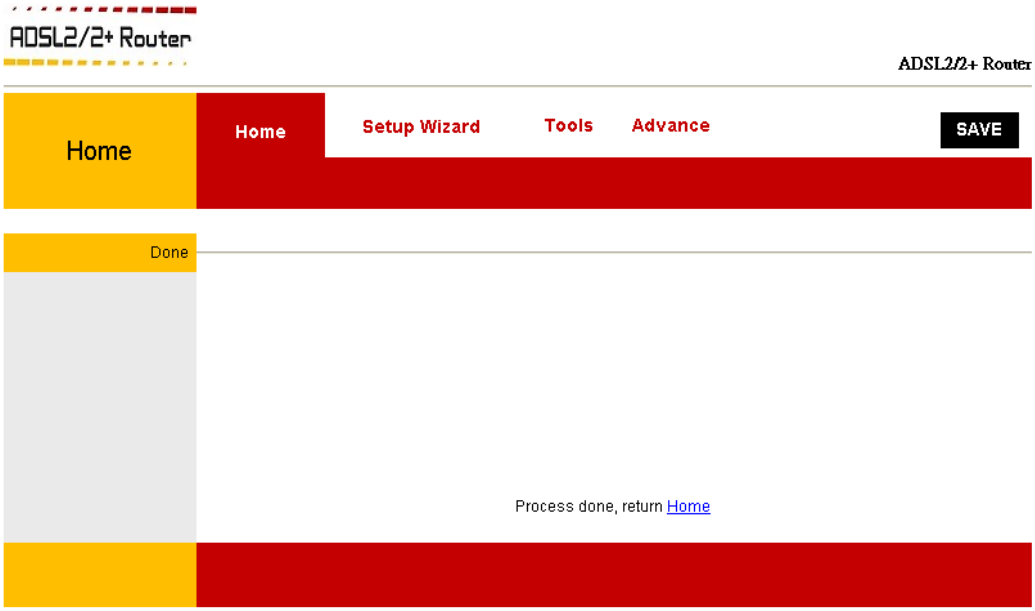
11. To make the change permanent, click on **SAVE**. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



12. The following window display indicates the save setting process.

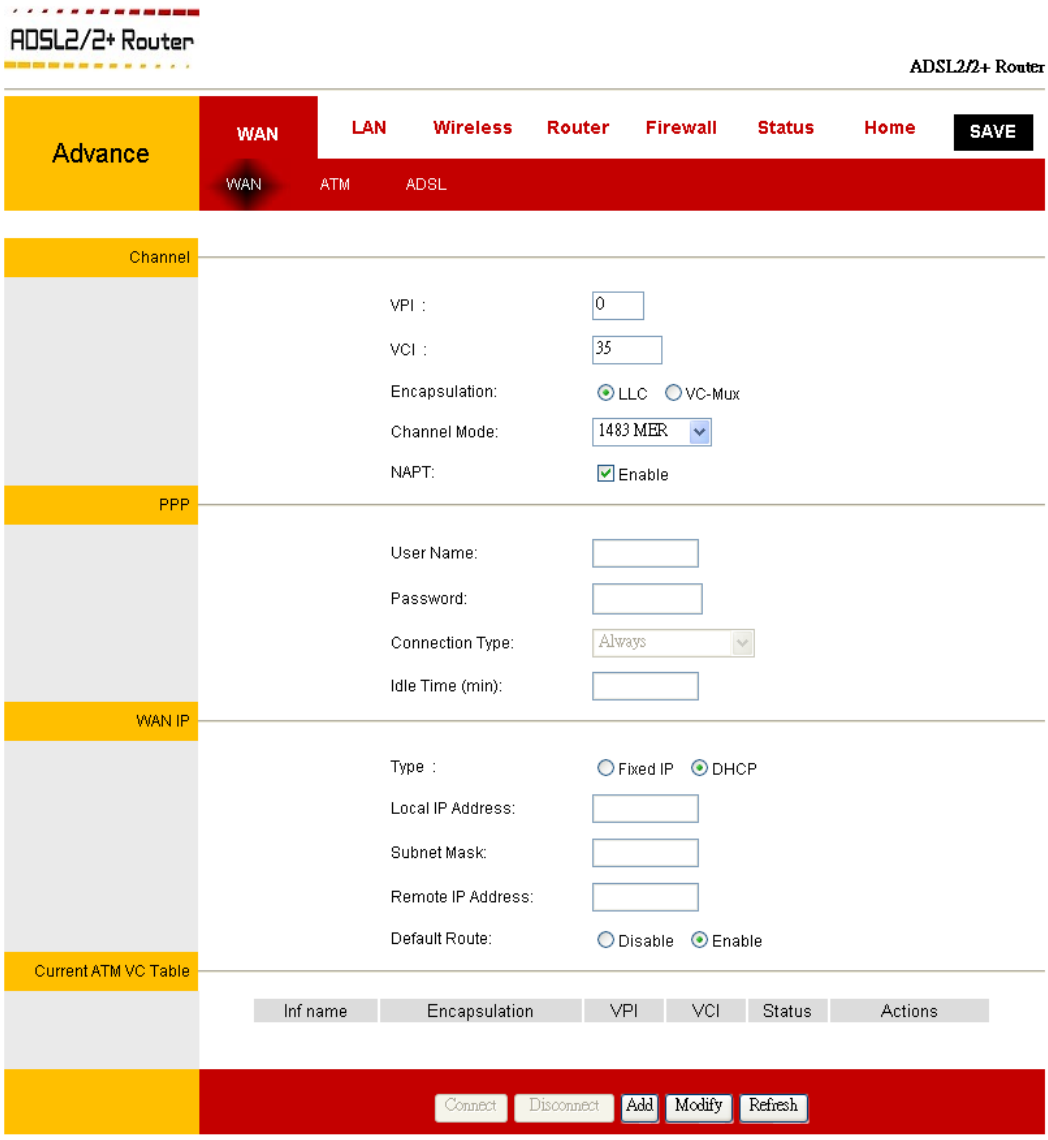


13. The following screen display after the save setting process. Click **Home** to get back to the System Home page. The System Home page will shows all the connection status and system information.



4.4.1.6.2 1483 MER Configuration Procedures – DHCP

1. From the **Advance – WAN – WAN** main page, click and select 1483 MER connection mode from the Channel Mode drop down manual. The default 1483 MER connection setup is displayed.



2. Under the **Channel** mode, enter the values of **VPI** and **VCI** settings.

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using 0,35.

3. Click the radio button and elect the Encapsulation type (LLC or VC-Mux).

   Note: Your ADSL service provider or your ISP will supply these. In this case the ADSL service provider is using LLC.

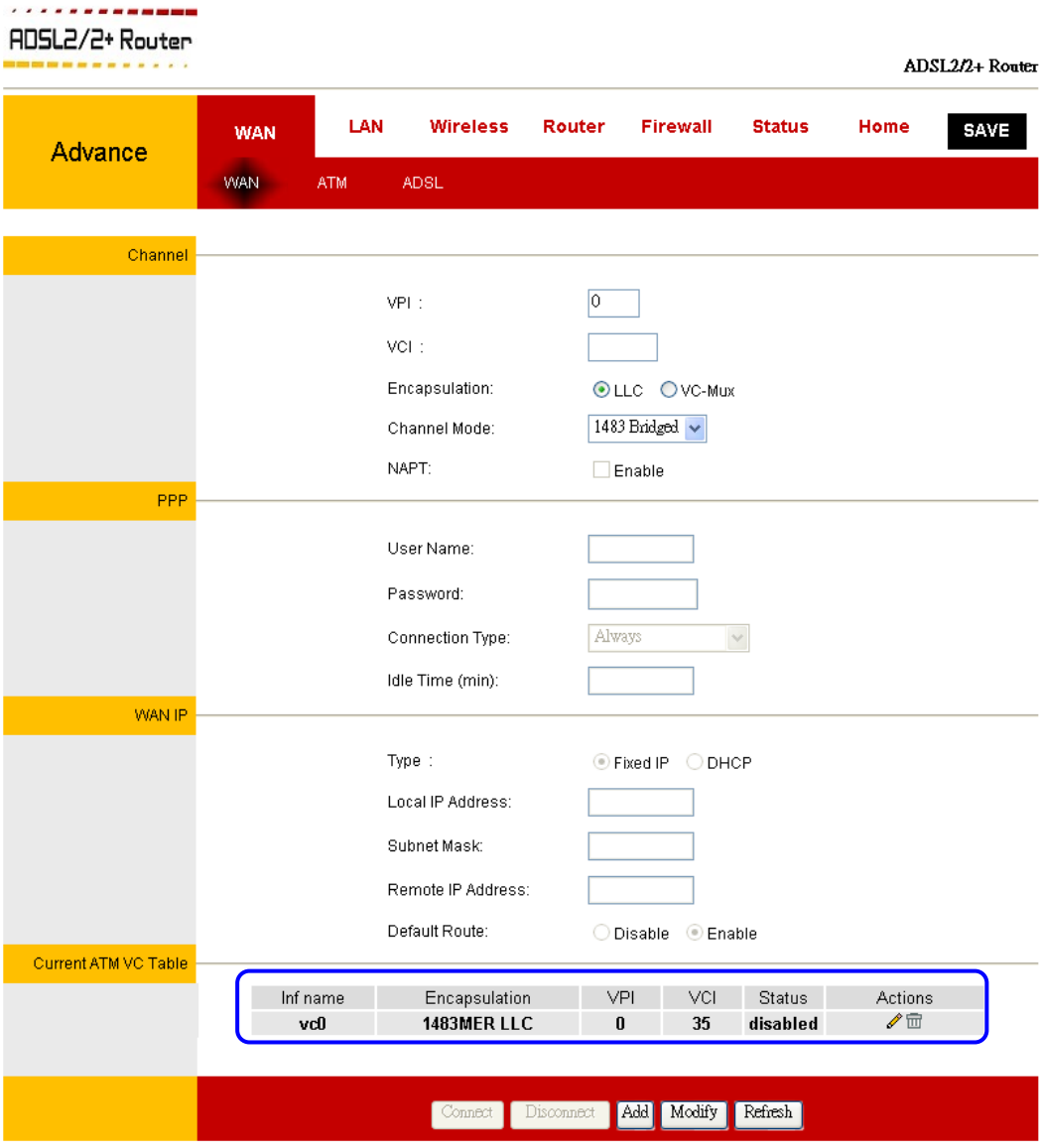
4. Check the radio button to **"Enable"** or **"Disable"** the NAPT setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

Note: **NAPT:** Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

5. Under the **WAN IP** mode, if you select DHCP as your connection type, nothing needed to fill. In this case the ADSL service provider is using Dynamic IP (Or DHCP) mode.

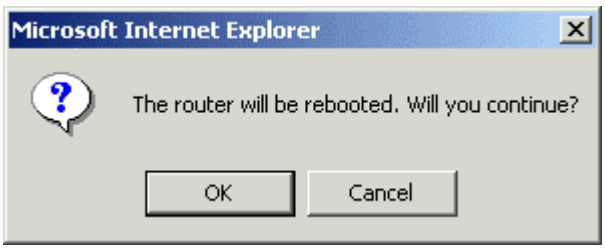
6. Check the radio button to **"Enable"** or **"Disable"** the Default Route setting. Leave as its default setting if your ADSL provider or ISP didn't provide any setting information.

7. Click **"Add"** button after setup. The following screen display:

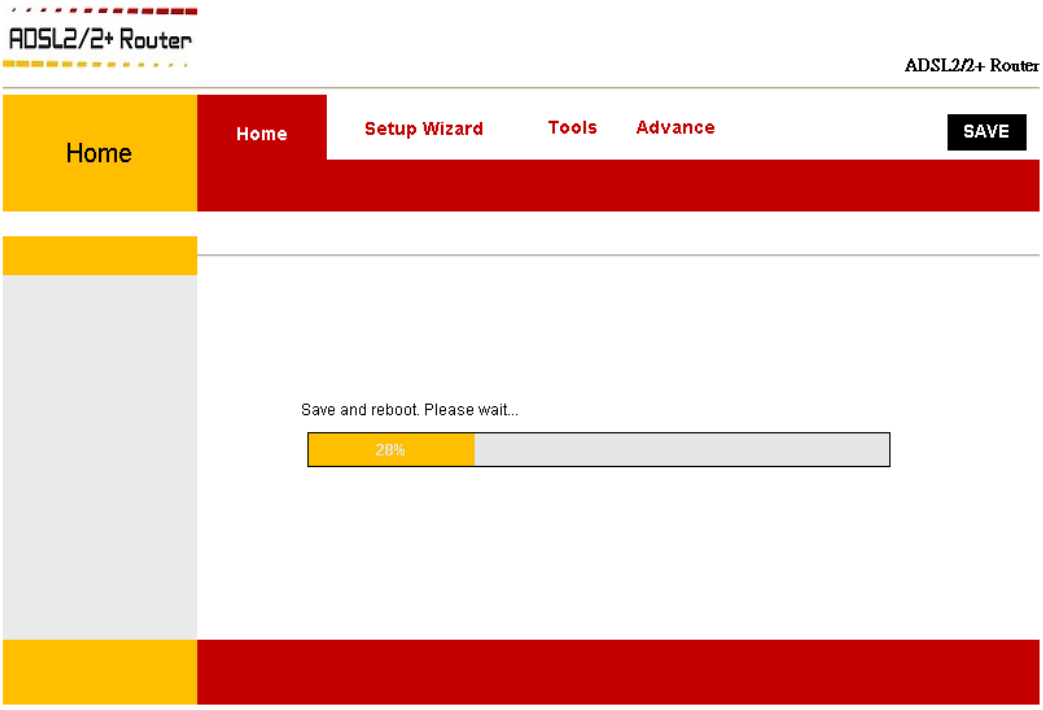


8. You can **"Edit"** ( ) or **"Delete"** ( ) the existing connection profile under the **Actions** column.

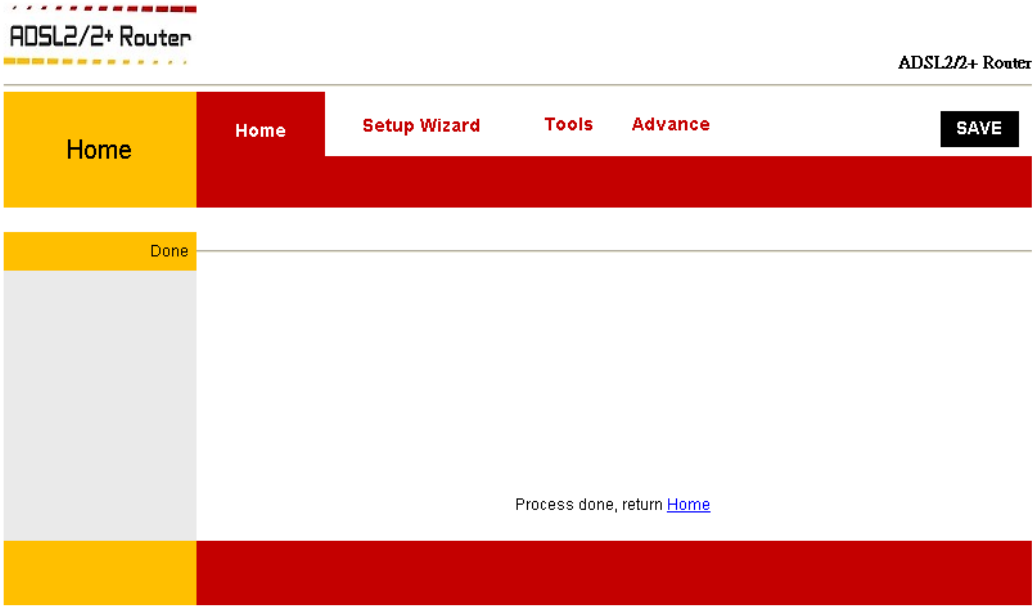
9. To make the change permanent, click on **SAVE**. The following wizard will pop-up after clicking the **"SAVE"** button. Click **"OK"** to confirm your setting.



10. The following window display indicates the save setting process.

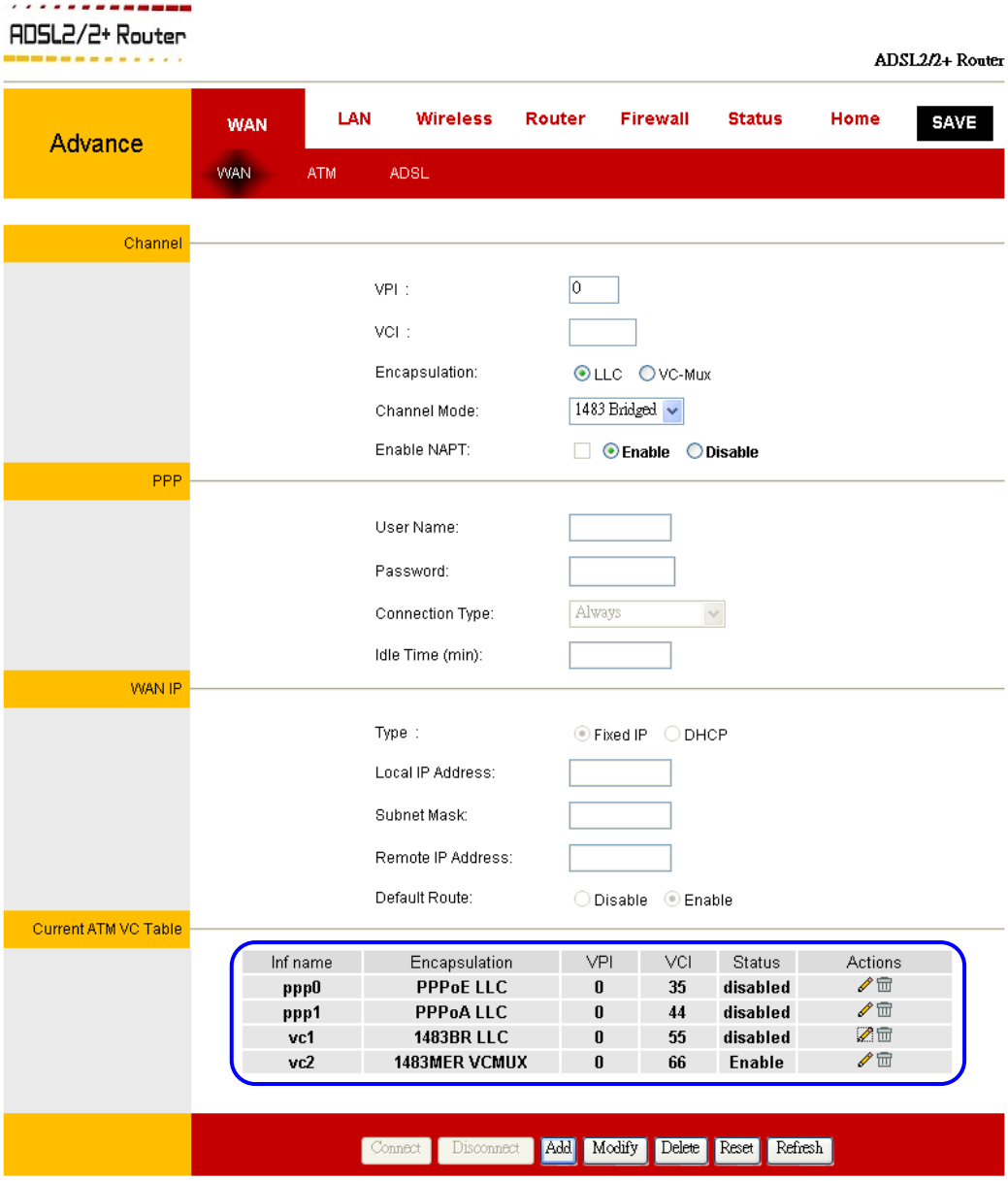


11. The following screen display after the save setting process. Click **Home** to get back to the System Home page. The System Home page will shows all the connection status and system information.



4.4.1.7 Edit Connection Profile

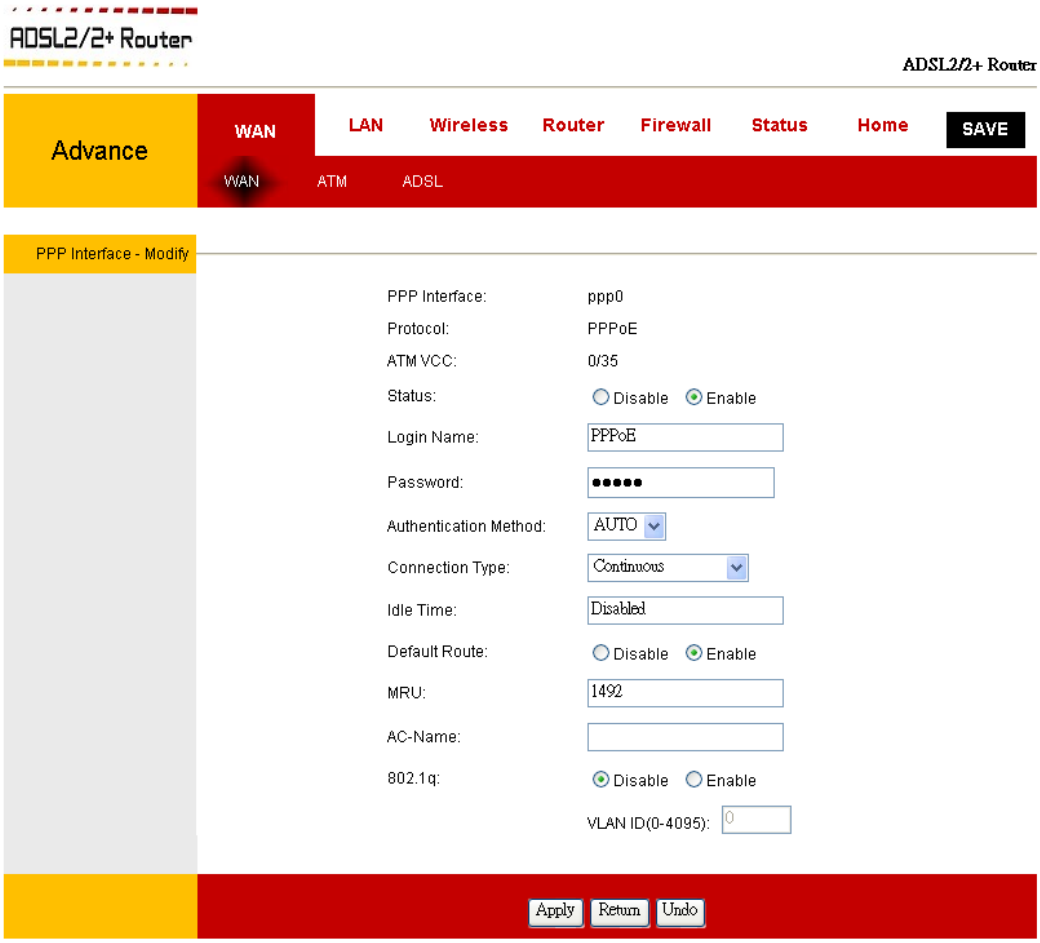
To view, modify, or delete an existing connection profile, display the **Advance – WAN – WAN** Configuration page, then click the Actions icons in the corresponding row in the connection profile table. To delete a connection profile from the table, click . To modify a connection profile from the table, click .



The following screen display when clicking the from the Actions column.

4.4.1.7.1 Edit Connection Profile – PPPoA & PPPoE User

The following screen display wneh clicking the under the Actions column for PPPoE or PPPoA connection.



- **PPP Interface:** States the interface that is being used. For PPPoA & PPPoE connection profile, the PPP Interface will named as ppp0, ppp1, ppp2…etc.
- **Protocol:** The Encapsulation type used for the connection.
- **ATM VCC:** The VPI & VCI setting for this connection profile.
- **Status:** Click “Enable” or “Disable” for this specific ADSL connection profile.
- **Login Name:** The PPPoE or PPPoA user name (provided by the ISP).
- **Password:** Enter the PPP password (provided by the ISP).

- **Authentication Method:** The different types of available authentications are:

  - ☑ **Auto:** When Auto is selected, PAP mode will run by default. However, if PAP fails, then CHAP will run as the secondary protocol. This is the default setting.
  - ☑ **PAP:** Password Authentication Procedure. Authentication is done through Username and Password.
  - ☑ **CHAP:** Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses Username and Password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

Connection Type: The PPP connection mechanism. There are 3 different Connection Type available for the PPP session:

- ☑ **Continuous:** The PPP connection session always on.
- ☑ **Connect on Demand:** The PPP connection will disconnect if no activity is detected after the specified Idle Time value. When checked, this field enables the Idle Time field.
- ☑ **Manual:** The PPP connection session start upon request.

- **Idle Time:** Specifies the PPP connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the **Connect on Demand** feature and is enabled only when the **Connect on Demand** field is checked. The default value is 600.

- **Default Route:** Click to “Enable” or “Disable” the Default Route features.

MRU: The MRU (Maximum Receive Unit) field indicates the maximum size IP packet that the peer of PPP connection (this device) can receive. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer’s MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

- **AC-Name:** Access Concentrator. Allows you to configure an Access Concentrator name for a PPPoE interface or connection profile. Leave as its default.

- **802.1q:** An IEEE standard for providing VLAN identification and quality of service (QoS) levels. When 802.1q feature is Enabled, you need to enter the VLAN ID (0 ~ 4095).

- **VLAN ID:** VLAN Identification. Multiple connections over the same PVC are supported, which requires the WAN network to have VLAN support and for the DSLAMS and Routers on the ISP to handle VLAN Tags.

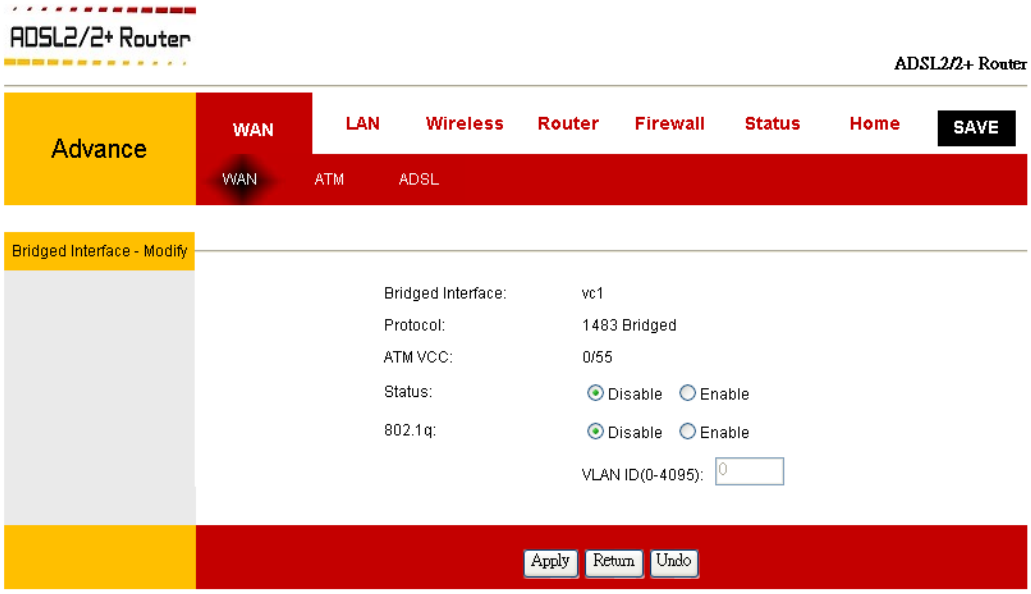
- **Apply:** Click Apply button after setup.

- **Return:** Click Return button and back to the Advance – WAN – WAN configuration page.

- **Undo:** Click Undo button for no changes.

4.4.1.7.2 Edit Connection Profile – 1483 Bridged/Routed/MER User

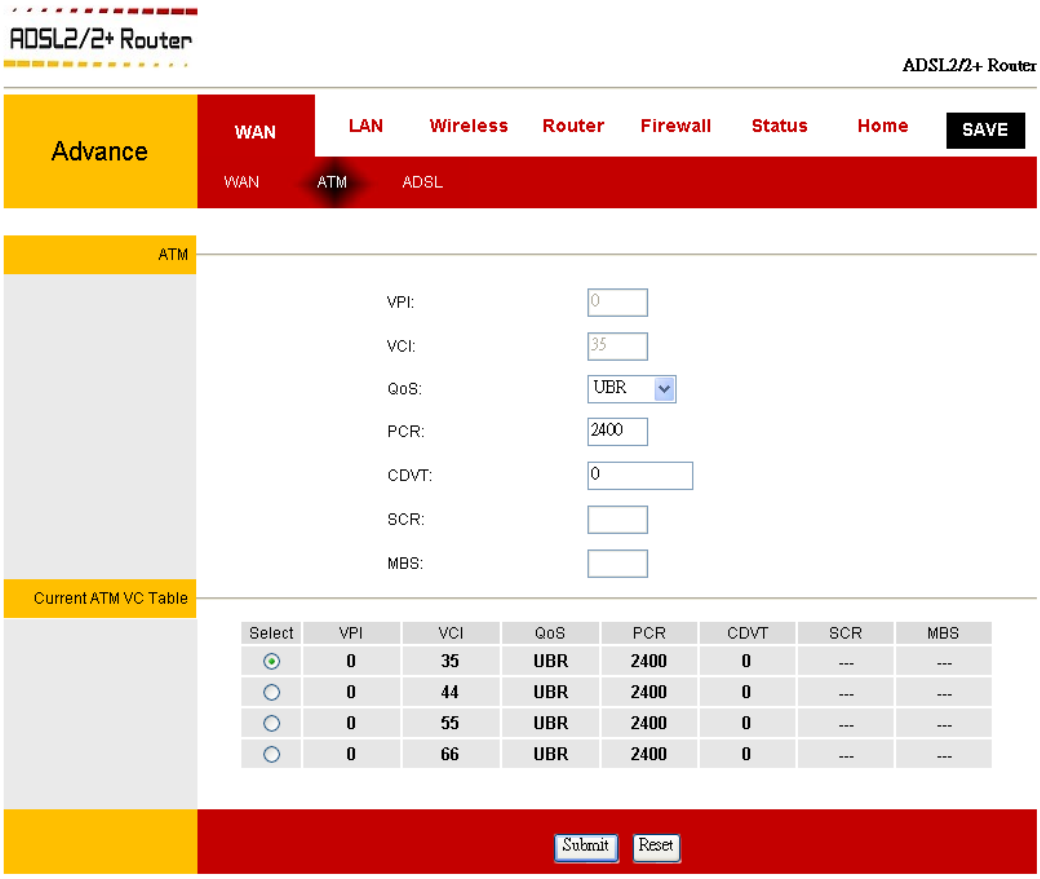
The following screen display wneh clicking the under the Actions column for PPPoE or PPPoA connection.



- **Bridged Interface:** States the interface that is being used. For 1483 Bridged, 1483 Routed & 1483 MER connection profile, the Bridged Interface will named as vc1, vc2, vc3…etc.
- **Protocol:** The Encapsulation type used for the connection.
- **ATM VCC:** The VPI & VCI setting for this connection profile.
- **Status:** Click “Enable” or “Disable” for this specific ADSL connection profile.
- **802.1q:** An IEEE standard for providing VLAN identification and quality of service (QoS) levels. When 802.1q feature is Enabled, you need to enter the VLAN ID (0 ~ 4095).
- **VLAN ID:** VLAN Identification. Multiple connections over the same PVC are supported, which requires the WAN network to have VLAN support and for the DSLAMS and Routers on the ISP to handle VLAN Tags.
- **Apply:** Click Apply button after setup.
- **Return:** Click Return button and back to the Advance – WAN – WAN configuration page.
- **Undo:** Click Undo button for no changes.

4.4.1.8 Advance – WAN – ATM

The **Advance – WAN – ATM** configuration page allows you to change or modify the ATM parameters.



- **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an 8-bit field in the ATM cell header. The VPI field specifies this 8-bit identifier for routing.

- **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16-bit numerical tag that determines the destination.

- **QoS:** Quality of service, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. If in doubt leave as default (UBR). The 4 **QoS** options are:

    - ☑ **UBR: Unspecified Bit Rate**. When UBR is selected, the PCR and CDVT fields are enabled.
    - ☑ **CBR: Constant Bit Rate**. When CBR is selected, the PCR and CDVT fields are enabled.
    - ☑ **nrt-VBR: Variable Bit Rate - non real time**. When nrt-VBR is selected, the PCR, SCR, MBS, and CDVT fields are enabled.

    - ☑ **rt-VBR: Variable Bit Rate - real time**. When rt-VBR is selected, the PCR, SCR, MBS, and CDVT fields are enabled.

- **PCR:** Peak cell rate, measured in cells/sec, is the cell rate which the source may never exceed.

- **CDVT:** Cell delay variation tolerance, the maximum amount of cell delay variation that can be accommodated. Cell delay variation measures the random inter-arrival times of cells within an ATM connection due to cell transfer delay caused by buffering, multiplexing, and so on.

- **SCR:** Sustained cell rate, measured in cells/sec, is the average cell rate over the duration of the connection.

- **MBS:** Maximum burst size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell Rate.

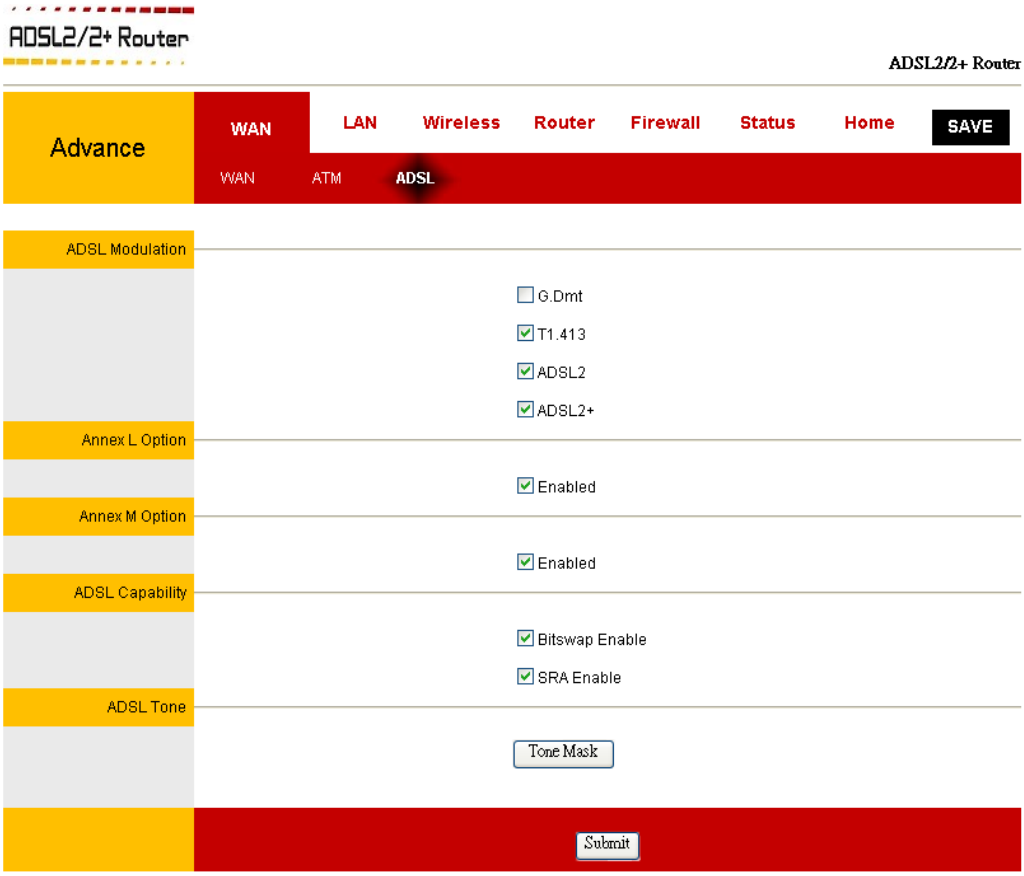
- **Submit:** Click Submit to confirm your setting.

- **Reset:** Click Reset to give up your changes.

4.4.1.9 Advance – WAN – ADSL

The **Advance – WAN – ADSL** configuration page show you the ADSL modulation type and allows you to select the modulation type from the list.

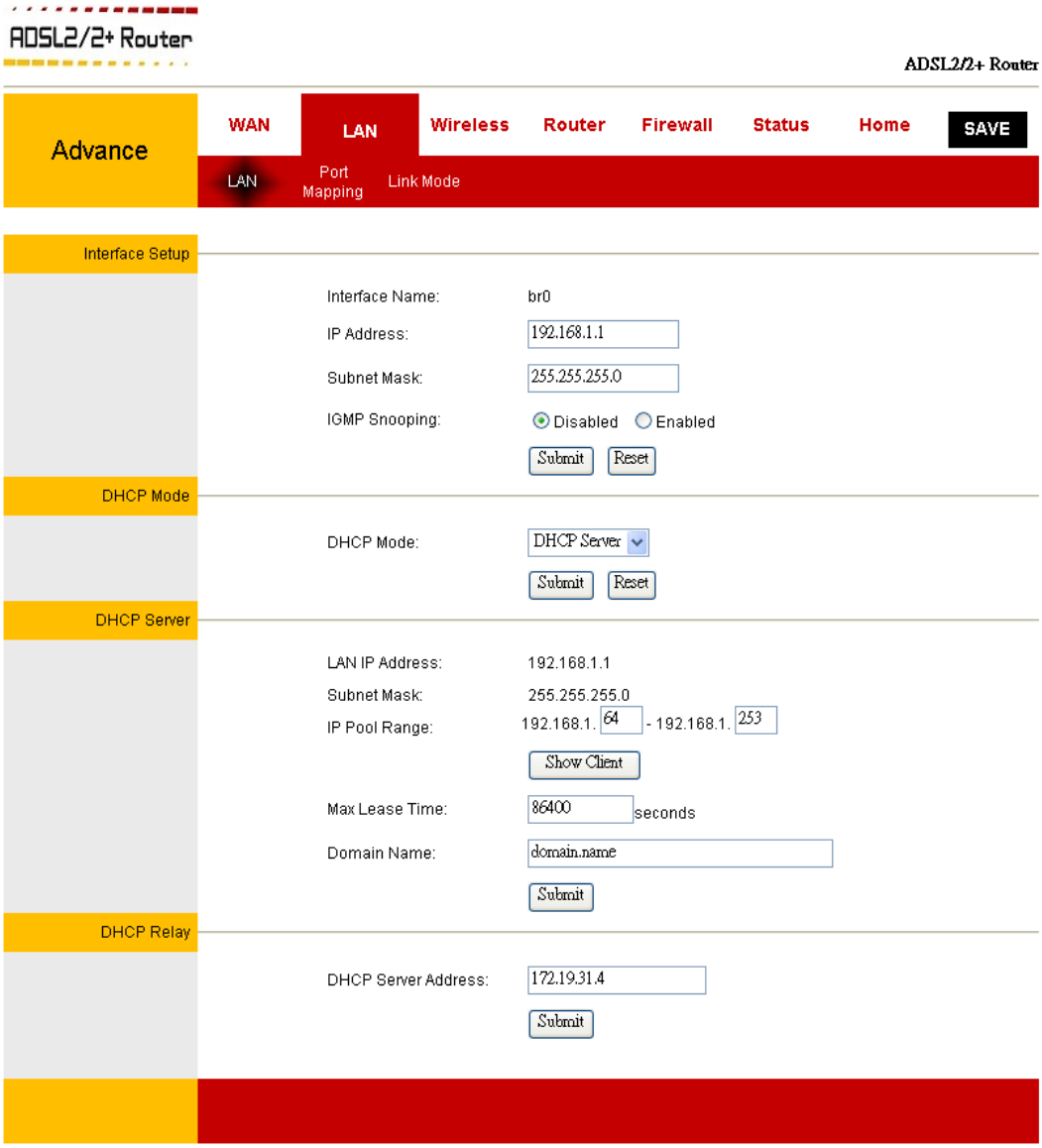
It's recommended that you leave the default value if you are unsure or the ISP/Telecom did not provide this information. For most all cases, this screen should not be modified.



4.4.2 Advance – LAN

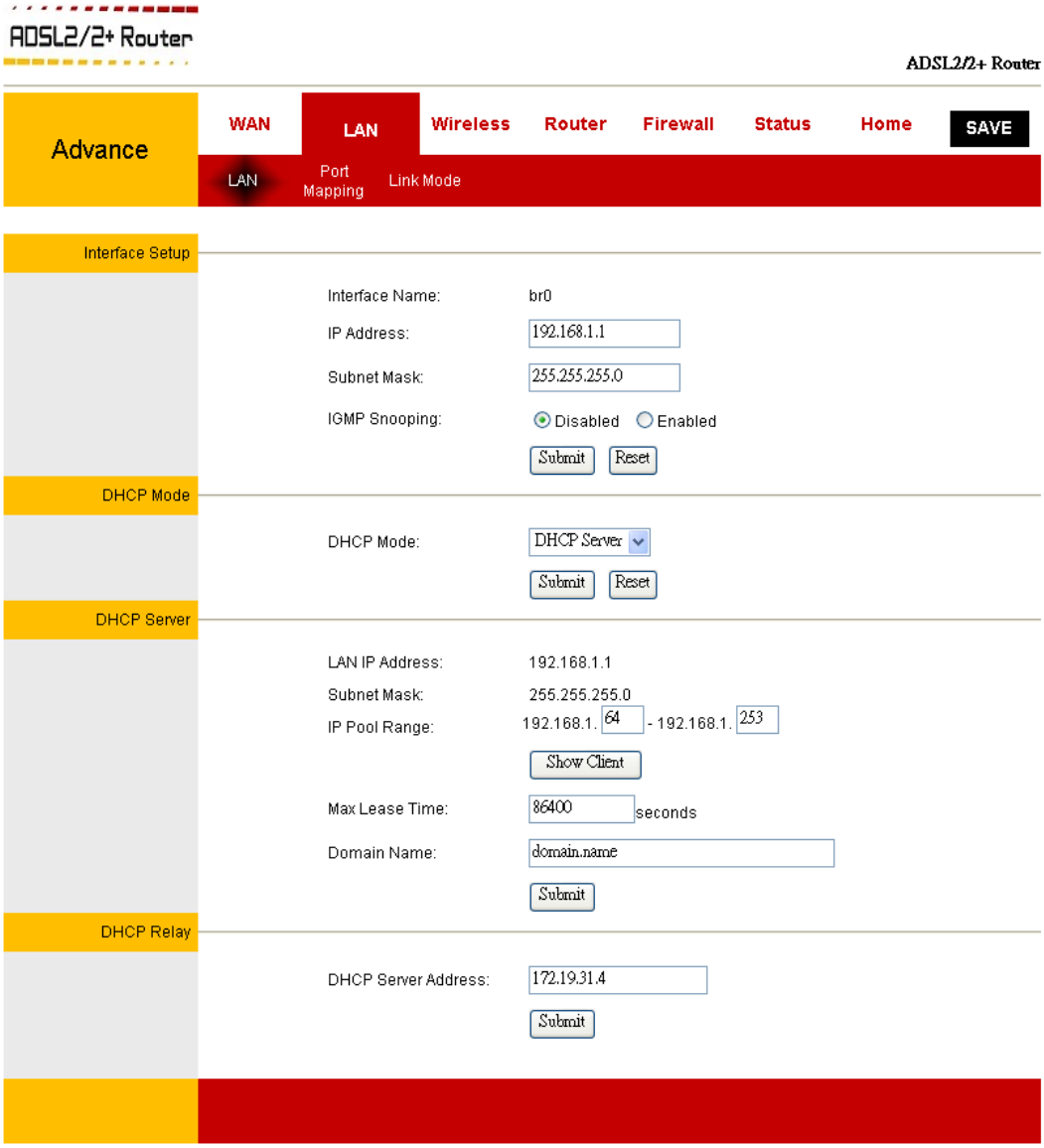
This section describes how to configure the interfaces on the 4 Ports ADSL2/2+ Router that communicate with your LAN computers. Click the **Advance – LAN** tab and the following **LAN** configuration homepage will pop-up.

If you are using the 4 Ports 11g Wireless ADSL2/2+ Router with multiple PCs on your LAN, you must connect the LAN via an Ethernet cable connected to the 4 Ports 11g Wireless ADSL2/2+ Router 's LAN port. Note that you must assign a unique IP address to each device interface that you use.



4.4.2.1 Advance – LAN – LAN

Click on the Advance – LAN – LAN tab, the following configurable screen display:



Refer to next page on the description of the LAN options.

■ Interface Setup:

- ☑ **Interface Name:** The LAN Interface name which is unchangeable.
- ☑ **IP Address:** The 4 Ports 11g Wireless ADSL2/2+ Router's IP address. The default IP address is 192.168.1.1.
- ☑ **Subnet Mask:** The default subnet mask of your 4 Ports 11g Wireless ADSL2/2+ Router is *255.255.255.0*. This subnet allows the 4 Ports 11g Wireless ADSL2/2+ Router to support 254 users. If you want to support a larger number of users you can change the subnet mask.
- ☑ **IGMP Snooping:** Allow the Ethernet Switch to check and make correct forwarding decisions. Default setting is **Disabled**.
- ☑ **Submit:** Click Submit to confirm your changes.
- ☑ **Reset:** Click Reset and give up any changes you'd made.

■ DHCP Mode:

DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network. When you enable DHCP on a network, you allow your ISP to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a **DHCP server**, and the receiving device is a **DHCP client**.

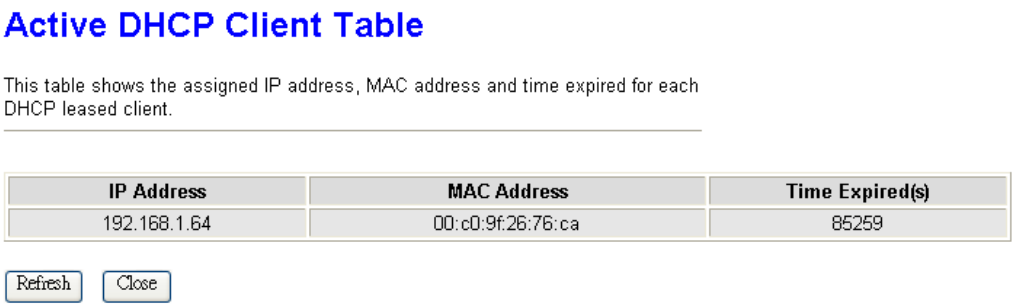
- ☑ **DHCP Mode:** Dynamic Host Configuration Protocol (DHCP) is a communication protocol that allows network administrators to manage and assign IP addresses to computers within the network. From the DHCP Mode drop-down list, choose **DHCP Server**, **DHCP Relay**, or **None**. If you choose none, your LAN computers must be configured with static IP addresses.
- ☑ **Submit:** Click Submit to confirm your cahnges.
- ☑ **Reset:** Click Reset and give up any changes you'd made.

■ DHCP Sever:

The DHCP server draws from a defined pool of IP addresses and **"Leases"** them for a specified amount of time to your computers when they connect to the network. It monitors, collects, and redistributes the addresses as needed.

- ☑ **LAN IP Address:** The 4 Ports 11g Wireless ADSL2/2+ Router's IP Address.
- ☑ **Subnet Mask:** Specifies which portion of each IP addresses in this range refers to the network and which portion refers to the host (computer). You can use the net mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (call a subnet).

- ☑ **IP Pool Range:** Specify the lowest and highest addresses in the pool. The default Start IP Address and End IP Address is 192.168.1.64 ~ 192.168.1.253.
- ☑ **Max Lease Time:** The amount of time left for the device to use the assigned address. The default lease time is 86400 seconds.
- ☑ **Domain Name:** A user-friendly name that refers to the subnet that includes the addresses in this pool.
- ☑ **Submit:** Click Submit to confirm your changes.
- ☑ **Show Client:** Click the Show Client button, the following Active DHCP Client Table display. Click **"Refresh"** to reload the window screen or click **"Close"** to close the DHCP Client Table.



■ DHCP Relay:

Some ISPs perform the DHCP server function for their customers' home/small office networks. In this case, you can configure the device as a **DHCP Relay** agent. When a computer on your network requests Internet access, the 4 Ports ADSL2/2+ Router connects your ISP to obtain an IP address and other information, and then forwards that information to the computer.

- ☑ **DHCP Server Address:** Type the IP address of your ISP's DHCP server.

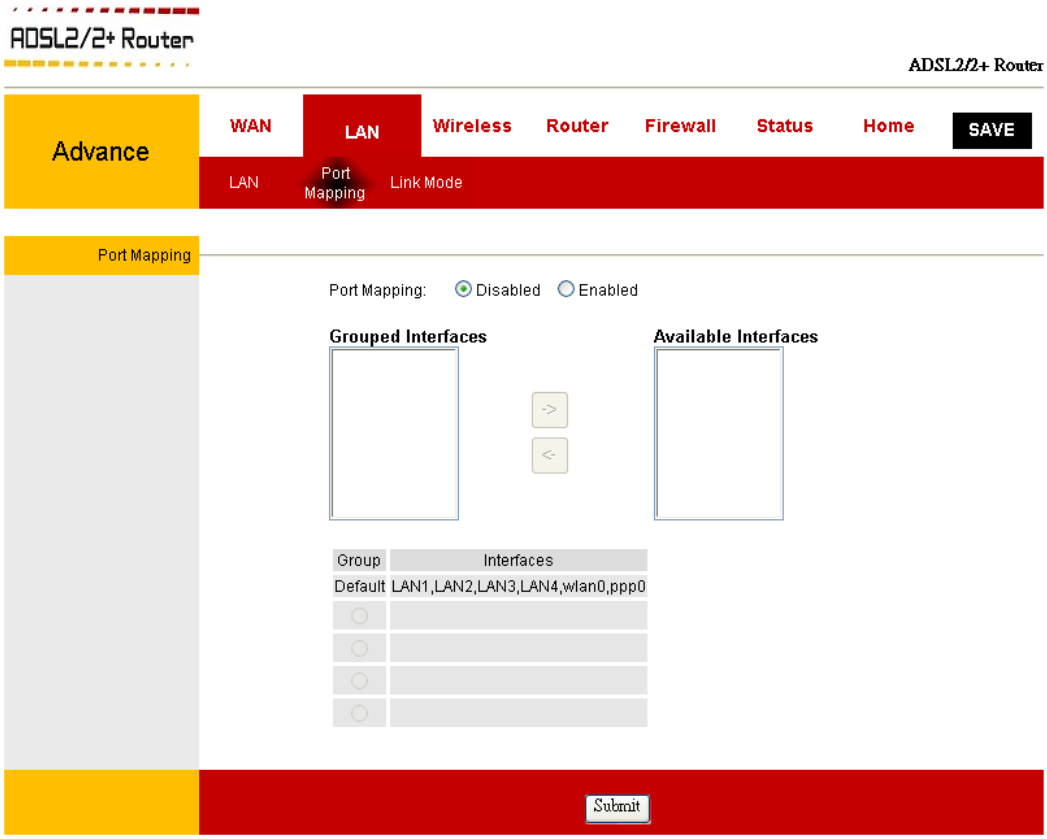
  If you do not have this address, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

- ☑ **Submit:** Click Submit to confirm your changes.

4.4.2.2 Advance – LAN – Port Mapping

Port Mapping is an advanced feature that allows servers to be hosted securely behind NAT. Internet servers listen on well-known ports for uninitiated connections. In other words, the server does not know in advance where a connection may come from. Examples of well-known ports include HTTP (TCP port 80), SMTP (TCP port 25), Telnet (TCP port 23). If these types of well-known services should be available to the Internet, then port mapping must be used to allow NAT to make exceptions for these services by redirecting these inbound connections to the appropriate local server.

Click **Advance – LAN – Port Mapping** tab, the following configuration homepage display.

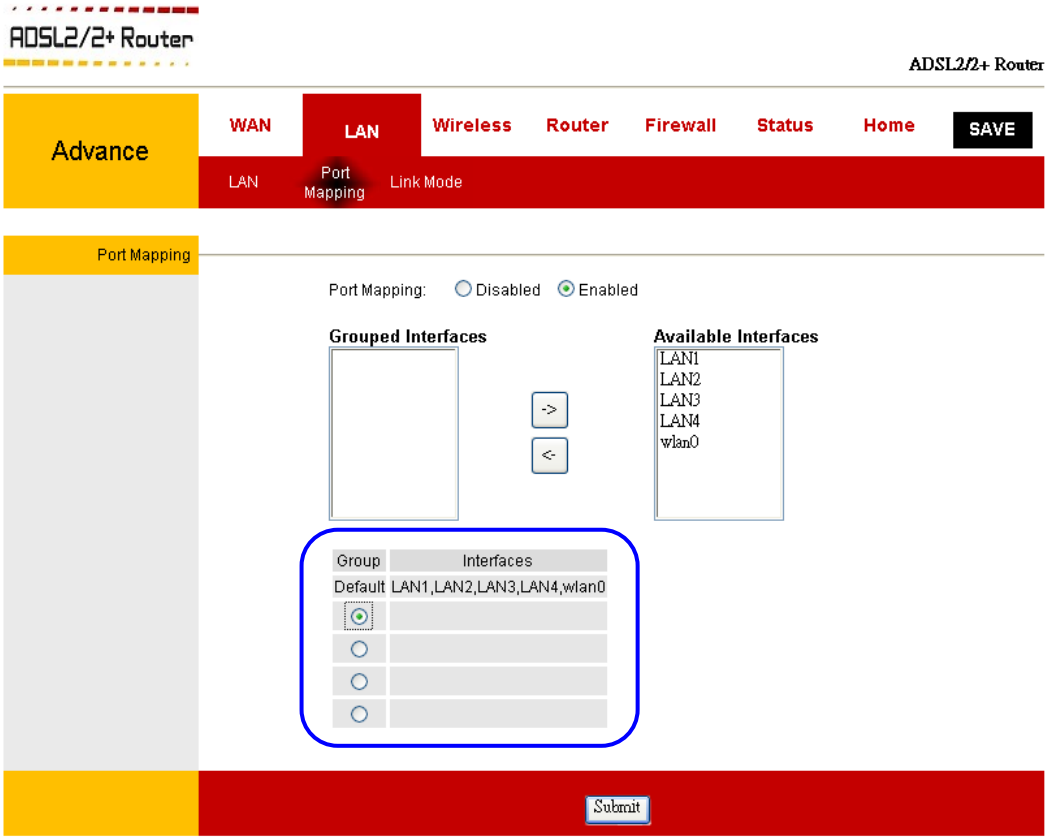


- **Port Mapping:** Click the radio button to **Enabled** or **Disabled** Port Mapping feature.
- **Grouped Interfaces:** Show the Grouped Interface.
- **Available Interfaces:** Show the Available Interfaces to grouped.
- **Submit:** Click Submit to confirm your setting.

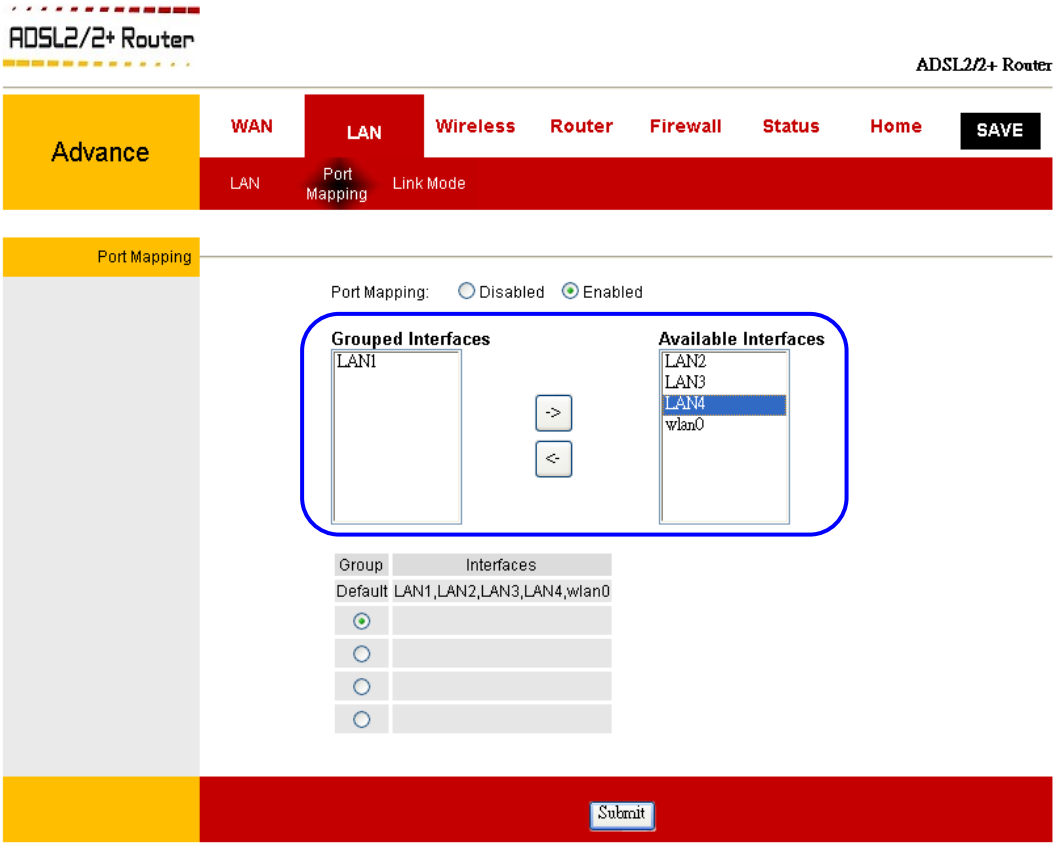
4.4.2.2.1 Port Mapping Configuration Procedures

1. From the **Port Mapping** configuration screen, click the radio button to **Enabled** Port Mapping feature.

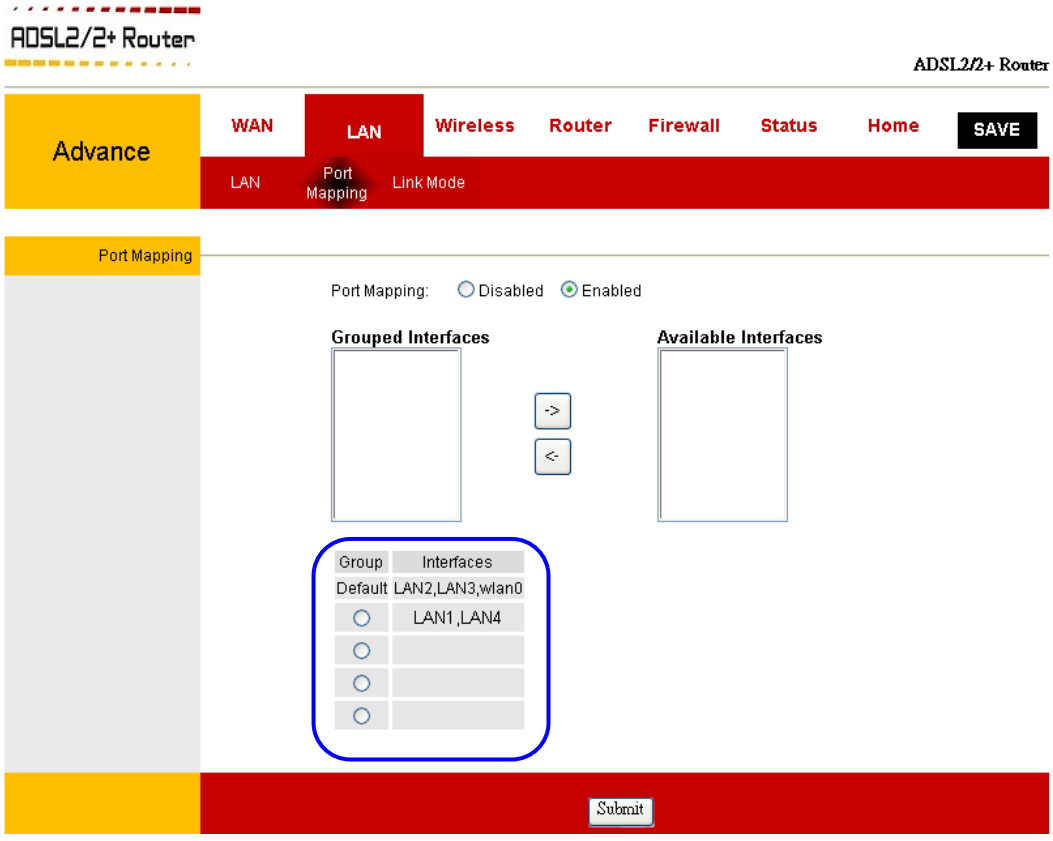
2. Click the group table's radio button, all the device interfaces will be listed under the **Available Interfaces** table as shown below.



3. Click the **Available Interfaces** listed then click the **"→"** or **"←"** tab to add or delete the interface to and fro from the **Grouped Interfaces** and **Available Interfaces** column. The following screen display.



4. Click Submit after setup. A **Change setting successfully!** Screen display. Click **"OK"** to confirm your setting and return back to the Port Mapping configuration page. The following screen display.

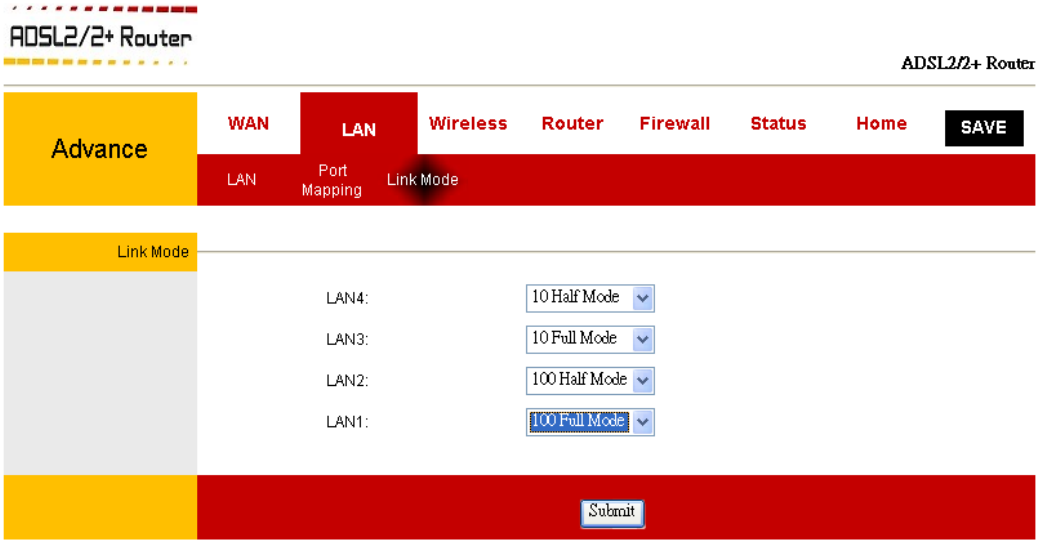


5. The selected Interface has been **Grouped**. Repeat the above procedures to **Grouped** the Interfaces upon your need.

4.4.2.3 Advance – LAN – Link Mode

The **Advance – LAN – Link Mode** settings can be configured to meet the requirements of your LAN configuration. As seen in the drop down menu in figure below, LAN setting options include:

- ☑ Auto Mode (default)
- ☑ 10 Half Mode
- ☑ 10 Full Mode
- ☑ 100 Half Mode
- ☑ 100 Full Mode



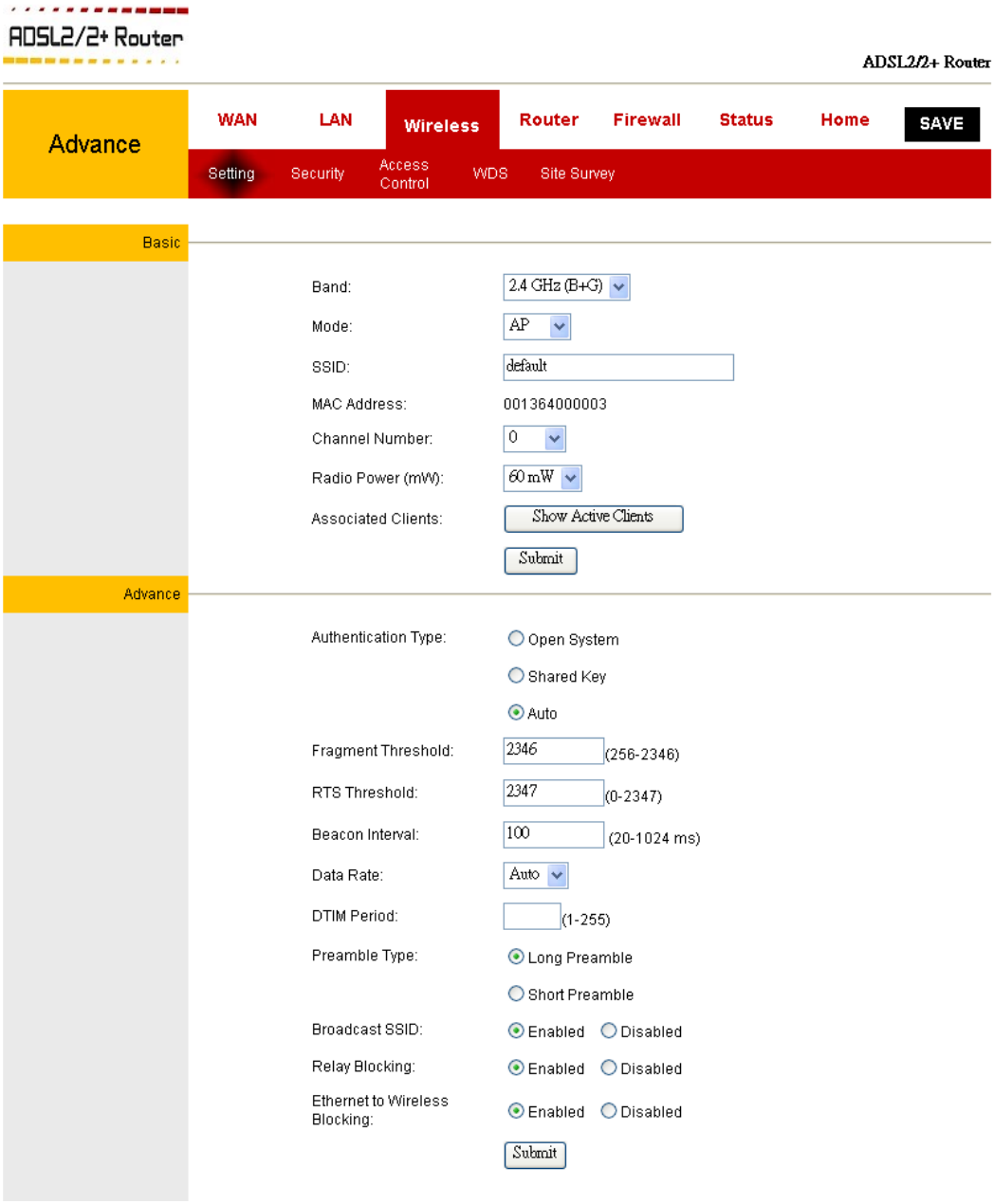
- **Auto Mode:** The 4 Ports 11g Wireless ADSL2/2+ Router will automatically sense which mode to use, selecting between 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex, and 10 Mbps Half Duplex. Default setting is **"Auto"**.

- **10 Half Mode:** Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 10Mbps.
- **10 Full Mode:** Data can be transferred and received simultaneously at the transfer rate of 10Mbps.
- **100 Half Mode:** Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 100Mbps.
- **100 Full Mode:** Data can be transferred and received simultaneously at the transfer rate of 100Mbps.
- **Submit:** Click **Submit** to complete the setting.

4.4.3 Advance – Wireless

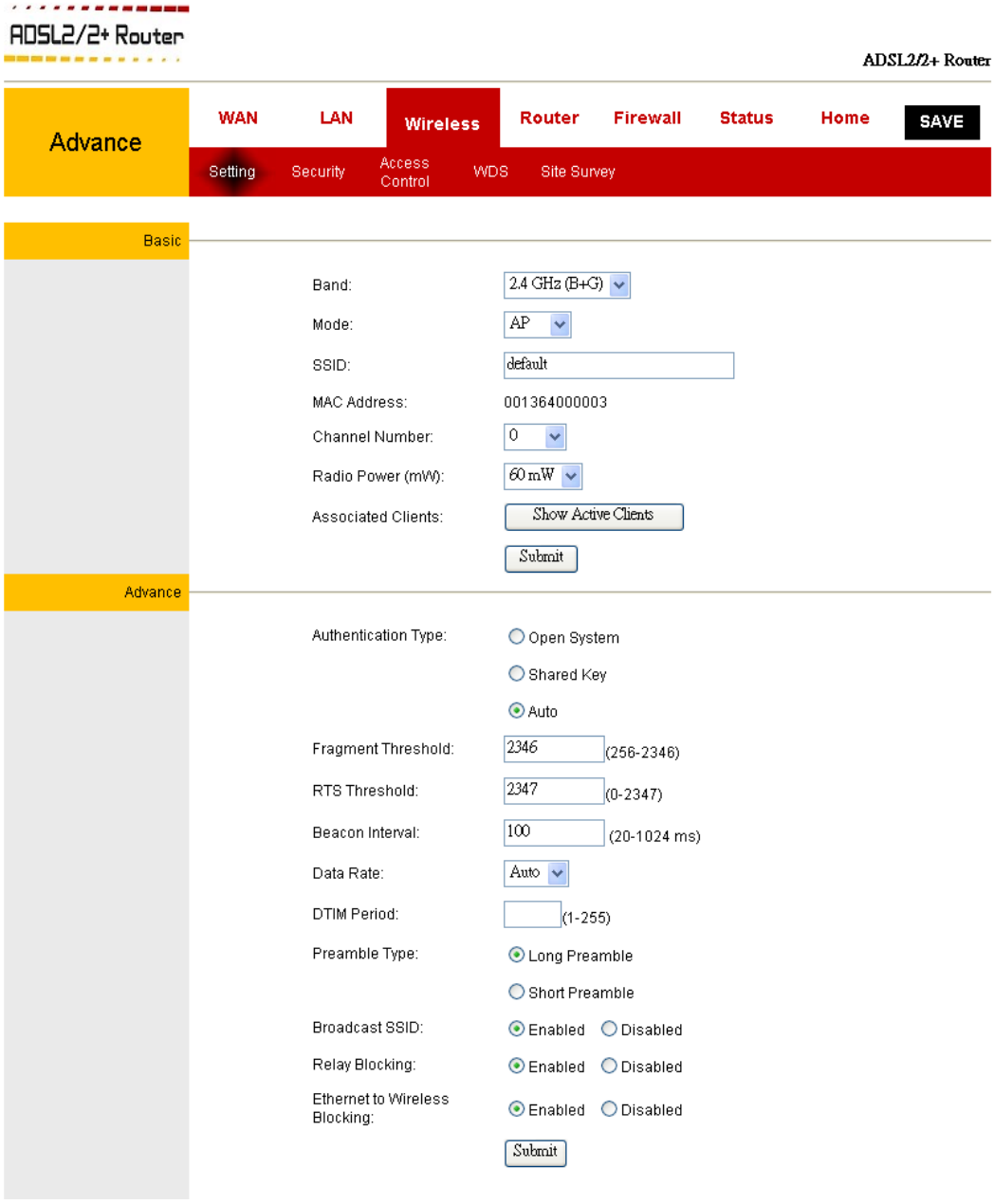
The Wireless configuration page describe the detail instruction on Setup, Configuration, Channel Range, Security and Management for Wireless network users.

Click on **Advance – Wireless** tab, the following **Wireless s**etting screen display.



4.4.3.1 Advance – Wireless – Setting

The **Advance – Wireless – Setting** configuration page describe the basic wireless setting for the 4 Ports 11g Wireless ADSL2/2+ Router. This screen provides basic local and Wireless networks parameter settings.



■ Basic:

☑ **Band:** The default is **"2.4 GHz (B+G)"**, which allows both 802.11g and 802.11b wireless stations to access this 4 Ports 11g Wireless ADSL2/2+ Router. You can select 2.4 GHz (B+G), 2.4 GHz (B) or 2.4 GHz (G) mode from the drop down manual.

☑ **Mode:** Select **"AP"**, **"Client"** or **"WDS"** mode from the drop down manual.

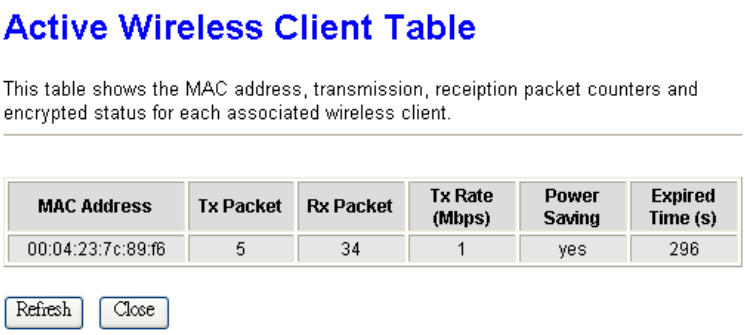
☑ **SSID:** The Service Set Identifier, also known as the Wireless Network name. The Service Set Identifier (SSID) is a unique name for your wireless network. If you have other wireless access points in your network, they must share the same SSID.

☑ **MAC Address:** The AP MAC Address.

☑ **Channel Number:** The channel on which the AP and the wireless stations will communicate. Different domain will have different ranges of channels.

☑ **Radio Power (mW):** The AP Radio Power. Select 60mW, 30mW or 15mW power level from the drop down manual. The default Radio Power level is 60mW. It's recommended to leave this setting as its default.

☑ **Associated Clients:** Click the **"Show Active Clients"** button, the following screen display:



The Active Wireless Clients Table shows the MAC Address, Receiption Packet Counters and Encrypted Status for each Associated Wireless Client.

☑ **Submit:** Click Submit button after setup.

■ Advance:

☑ **Authentication Type:** Authentication algorithm to use when the security configuration is set to Legacy. When the security configuration is set to 802.1x or WPA, the authentication algorithm is always open. This field is enabled when the WEP security field is checked. There are three options:

- ◆ **Open System:** In open-system authentication, the access point accepts any station without verifying its identify.
- ◆ **Shared Key:** Shared-key authentication requires a shared key (WEP encryption key) be distributed to the stations before attempting authentication.
- ◆ **Auto:** If Auto is selected, the access point will perform shared-key authentication, then open-system authentication.

- ☑ **Fragment Threshold:** The Fragmentation Threshold. The range is 256 ~ 2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended. This default setting is 2346. However, when 4x is enabled on the setup page, the fragmentation threshold value changes to 4096.
- ☑ **RTS Threshold:** The range is 0 ~ 2347 bytes. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The 4 Ports 11g Wireless ADSL2/2+ Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. This default setting is 2347.
- ☑ **Beacon Interval:** Enter a value between 20 ~ 1024 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the 4 Ports 11g Wireless ADSL2/2+ Router to synchronize the wireless network. The default value is 100.
- ☑ **Data Rate:** Select the Wireless Data Rate. The default setting is **"Auto"**.
- ☑ **DTIM Period:** This value, between 1 ~ 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the 4 Ports 11g Wireless ADSL2/2+ Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
- ☑ **Preamble Type:** Select **"Always Long Preamble"** or **"Long/Short Preamble"**. The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless router and the roaming wireless network adapters.
- ☑ **Broadcast SSID:** Enable or Disable Broadcast SSID functionality. The default setting is **"Enabled"**.
- ☑ **Relay Blocking:** Enable or Disable Relay Blocking functionality. The default setting is **"Enabled"**.
- ☑ **Ethernet to Wireless Blocking:** Enable or Disable Ethernet to Wireless Blocking functionality. The default setting is **"Enabled"**.
- ☑ **Submit:** Click **Submit** to complete and confirm your setting.

4.4.3.2 Advance – Wireless – Security

The **Wireless – Security** page describes how to configure the Wireless Security Level of your 4 Ports 11g Wireless ADSL2/2+ Router. There are four security level (The **Encryption** drop down manual) provided by this 4 Ports 11g Wireless ADSL2/2+ Router:

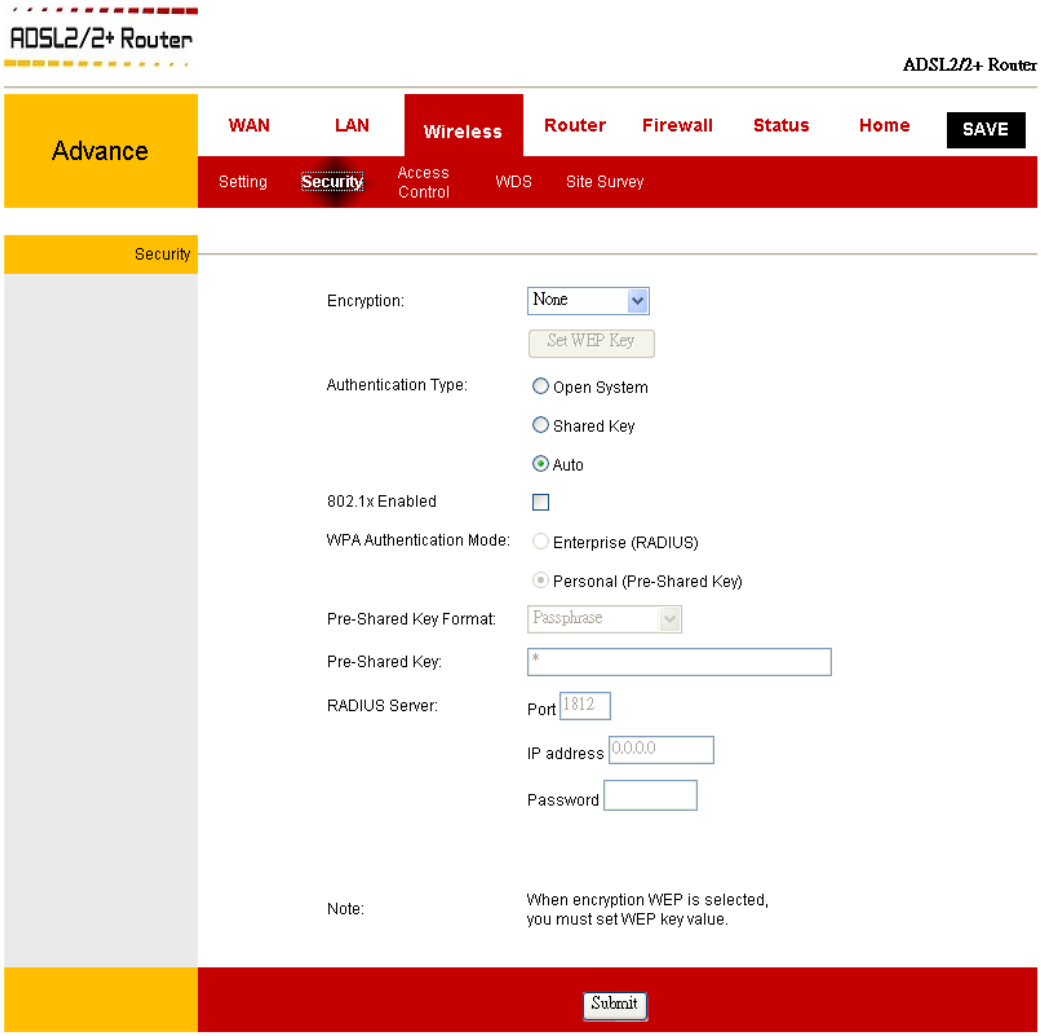
- **None:** No security used.

- **WEP (Wired Equivalent Privacy):** WEP is a security protocol for wireless local area networks defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

- **WPA (TKIP): WPA** is a security protocol for WLAN. WPA uses a sophisticated key hierarchy that generates new encryption keys each time a mobile device establishes itself with an AP. WPA uses temporal key integrity protocol (TKIP) for data encryption.

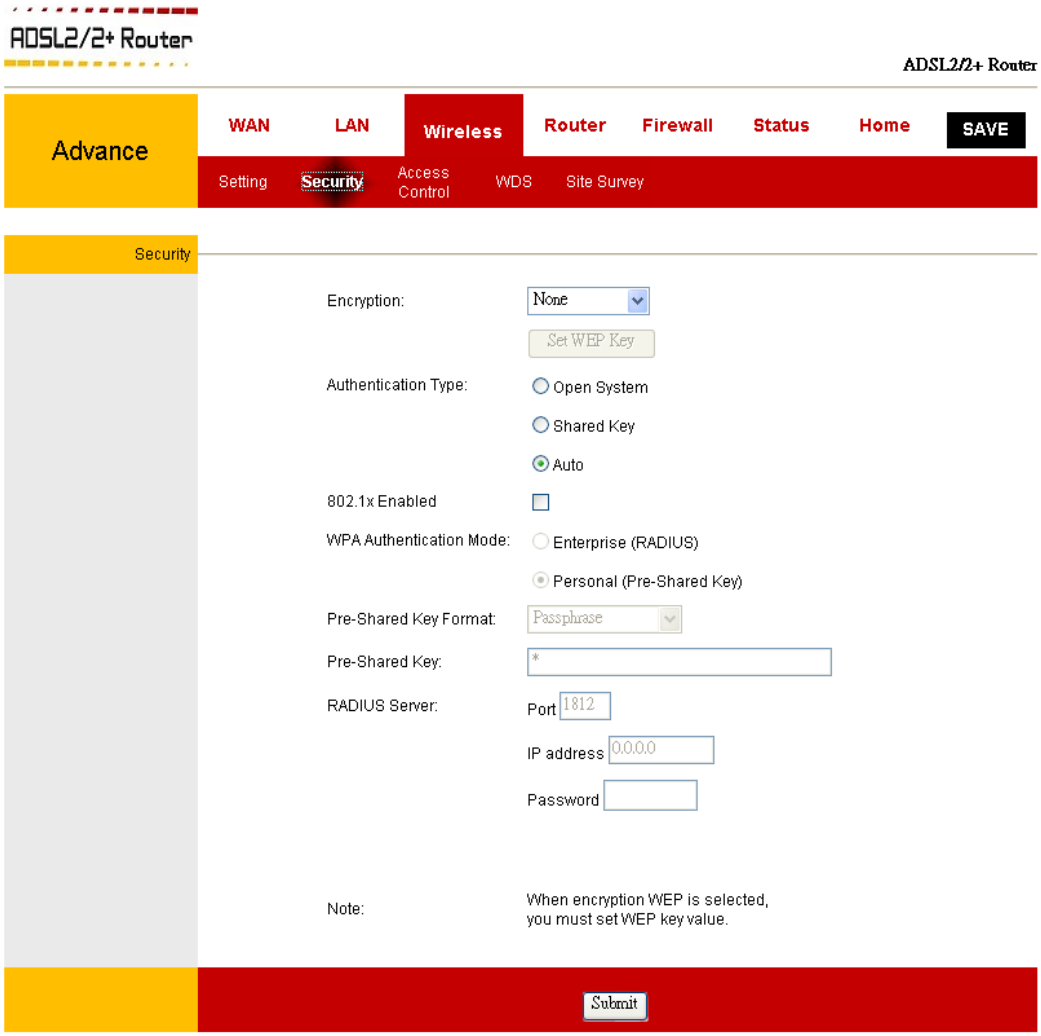
- **WPA2 (AES):** WPA2, also known as 802.11i, uses advanced encryption standard counter mode CBC-MAC protocol (AES-CCMP) for data encryption.

- **WPA2 Mixed:** Support both WPA and WPA2 encryption mechanism.


ADSL2/2+ Router
ADSL2/2+ Router
Advance
WAN
LAN
Wireless
Router
Firewall
Status
Home
SAVE
Setting
Security
Access Control
WDS
Site Survey
Security
Encryption:
None
Set WEP Key
Authentication Type:
Open System
Shared Key
Auto
802.1x Enabled
WPA Authentication Mode:
Enterprise (RADIUS)
Personal (Pre-Shared Key)
Pre-Shared Key Format:
Passphrase
Pre-Shared Key:
*
RADIUS Server:
Port
1812
IP address
0.0.0.0
Password
Note:
When encryption WEP is selected, you must set WEP key value.
Submit

4.4.3.2.1 Wireless Security – None

None: Wireless security is not used. No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed. The following screen display when selecting the **"None"** Encryption from the drop down manual:



- Click **"Submit"** after setup.

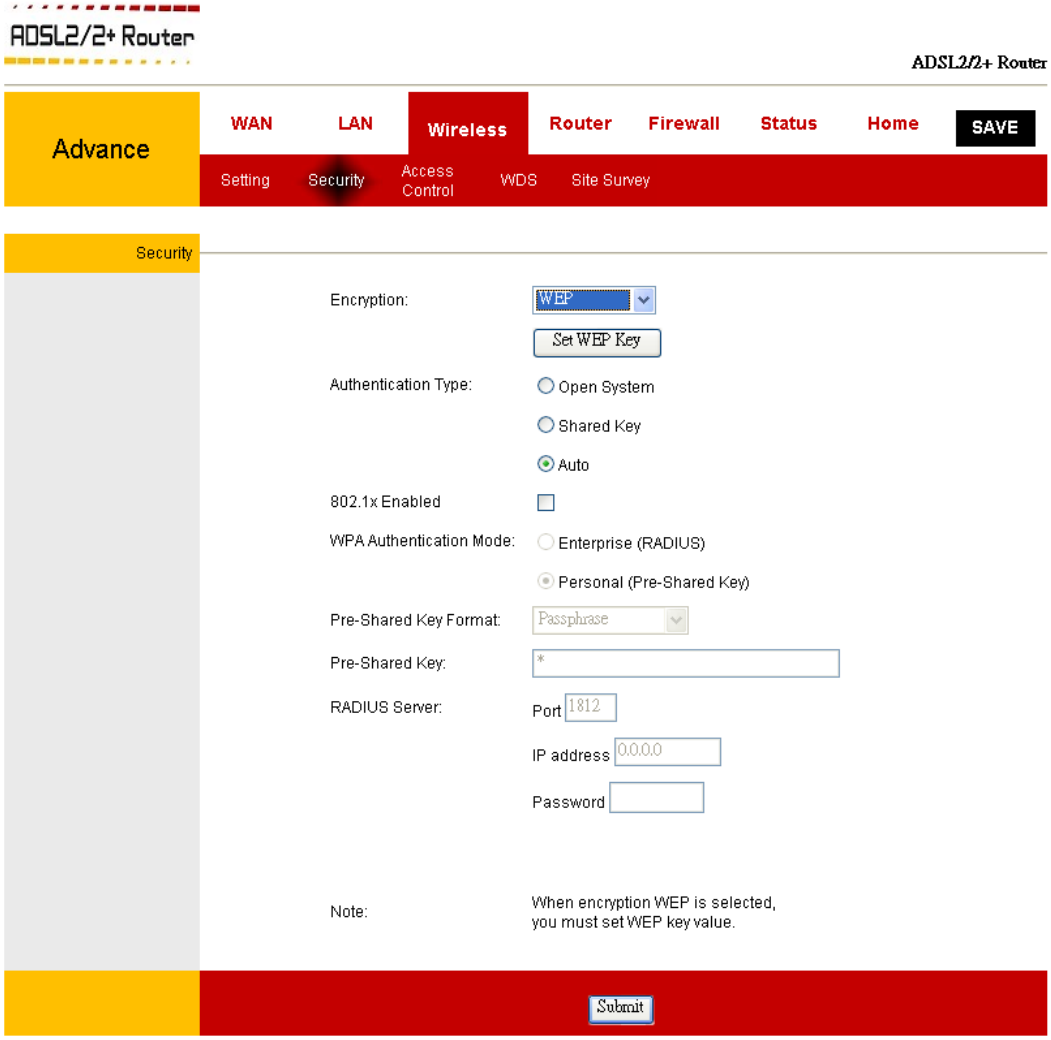
- To make the change permanent, click on **SAVE**.

4.4.3.2.2 Wireless Security – WEP

WEP: Wired Equivalent Privacy. WEP is a security protocol for wireless local area networks defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. The 4 Ports 11g Wireless ADSL2/2+ Router supports 2 levels of WEP encryption:

- 64 Bit encryption
- 128Bit encryption

With WEP, the receiving station must use the same key for decryption. Each radio NIC and access point, therefore, must be manually configured with the same key. Figure below illustrates the default setting of the WEP Wireless Security screen.



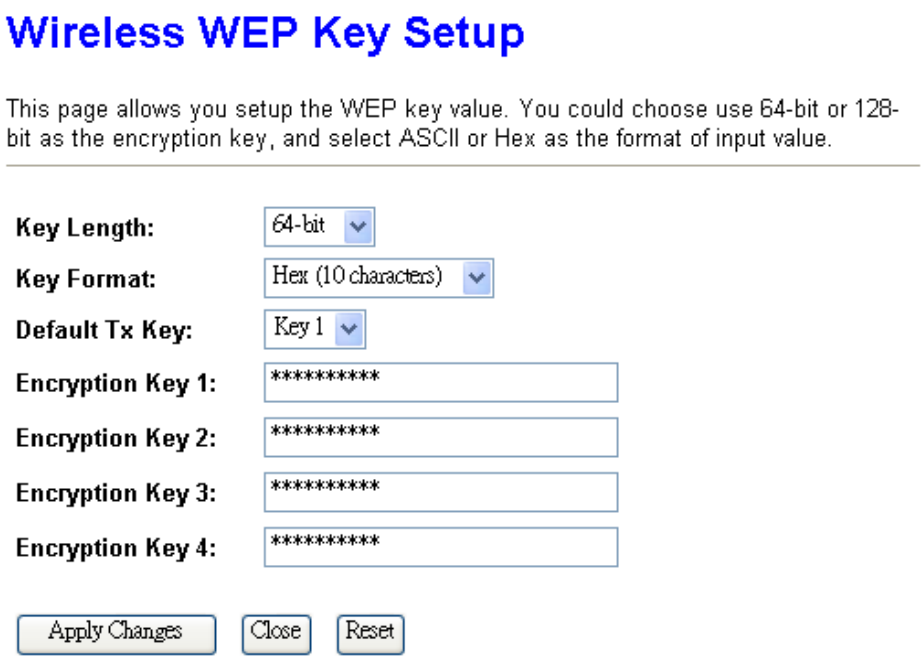
802.1x is a security protocol for Wireless Local Area Networks (WLAN). It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on Extensible Authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the RADIUS (Remote Authentication Dial-In User Service) protocol. When **802.1x** is used (Check to Enable), the following RADIUS Server's data have to be provided:

☑ **Port:** The protocol port of the RADIUS server.

☑ **IP address:** The IP address of the RADIUS server. Used for authentication.

☑ **Password:** The Password that the AP shares with the RADIUS server.

- **Set WEP Key:** Click the **"Set WEP Key"** button, the following screen display:



- **Key Length:** Choose between **64-bit** (default) and **128-bit**. 128-bit offers more security, but at the cost of slower packet processing.

  ☑ For **64-bit** WEP Key Length, enter 10 Hexadecimal digits or 5 Characters (any combination of 0~9, A~F).

  ☑ For **128-bit** WEP Key Length, enter 26 Hexadecimal digits or 13 Characters (any combination of 0~9, A~F).

- **Key Format:** Check and select the **"Key Format"** from the drop down manual. Both **"Hex"** and **"ASCII"** format are supported.

- **Default Tx Key:** Select your **Default Tx Key** from the drop down manual.

- **Encryption Key:** Enter your WEP Encryption Key. You are able to enter 4 encryption keys, only one of which is enabled at any given time. All devices on the network must share the selected key in order to communicate with the 4 Ports 11g Wireless ADSL2/2+ Router. The key length for 64-bit is 10 hexadecimal characters and the key length for 128 bit is 26 hexadecimal characters.

- **Apply Changes:** Click **Apply Changes** to complete the setting.

- **Close:** Click **Close** to close the setup wizard.

- **Reset:** Click **Reset** to ignore all the changes.

4.4.3.2.2.1 Configure WEP

WEP is disabled by default. Use the following procedures to enable WEP on your access point.

1. Check and select **WEP** Encryption.

2. Click **"Set WEP Key"** button to set your WEP Key.

3. Select **"WEP Key Length"** (64-bit or 128-bit).

4. Select the **"WEP Key Format"** (Hex or ASCII Format).

5. Select your **"Default Tx Key"** (Key 1 ~ Key 4).

6. Enter **Encryption key** (Encryption Key 1 ~ Encryption Key 4).

7. Click to **"Enable"** or **"Disable"** 802.1x option. If 802.1x is **"Enabled"**, check and select WEP 64bits or WEP 128bits encryption. The following RADIUS Server's data have to be provided at the same time:

   - ☑ **Port:** The protocol port of the RADIUS server.
   - ☑ **IP address:** The IP address of the RADIUS server. Used for authentication.
   - ☑ **Password:** The Password that the AP shares with the RADIUS server.

8. Click **Apply Changes** to complete the setting.

9. The **"Change setting successfully!"** screen will pop-up. Click **"OK"** to confirm your setting.

10. Click **"Close"** to end the WEP setting wizard.

11. To complete and save the setting permanently, click **SAVE**.

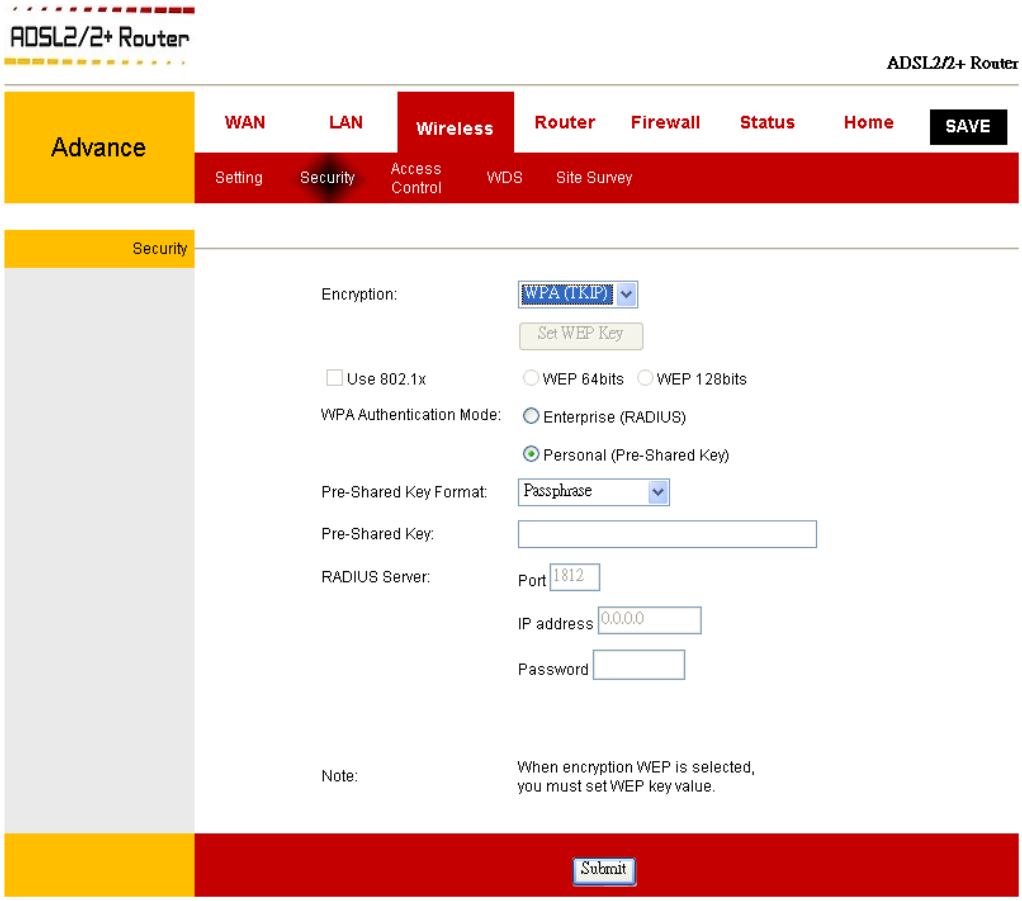
4.4.3.2.3 Wireless Security – WPA (TKIP)

WPA (Wi-Fi Protected Access) is the most dominating security mechanism in industry. **WPA** is a security protocol for WLAN. WPA uses a sophisticated key hierarchy that generates new encryption keys each time a mobile device establishes itself with an AP.

WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while **WPA2** applies AES. Protocols including 802.1X and RADIUS are used for strong authentication. Like WEP, keys can still be entered manually (pre-shared keys); however, using a RADIUS authentication server provides automatic key generation and enterprise-wide authentication. WPA uses temporal key integrity protocol (TKIP) for data encryption.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network.

Figure below shows the default setting of the **Wireless – Security – WPA (TKIP)** page.



- **Use 802.1x: 802.1x** is a security protocol for Wireless Local Area Networks (WLAN). It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on Extensible Authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the RADIUS (Remote Authentication Dial-In User Service) protocol. When **802.1x** is **"Enabled"** by default.

- **WPA Authentication Mode:** Click the radio button to enable **"Enterprise (RADIUS)"** or **"Personal (Pre-Shared Key)"** mode.

  ☑ **Enterprise (RADIUS) Mode:** When Enterprise (RADIUS) mode is check, the following RADIUS Server's data have to be provided at the same time:

  - **Port:** The protocol port of the RADIUS server.
  - **IP address:** The IP address of the RADIUS server. Used for authentication.
  - **Password:** The Password that the AP shares with the RADIUS server.

  ☑ **Personal (Pre-Shared Key) Mode:** A Pre-Shared Key identifies a communication party during the IKE negotiation. It is called **"Pre-Shared"** because you have to share it with another party before you can communicate with them over a secure connection. Click and select your **"Pre-Shared Key Format"**. Two different format are provided:

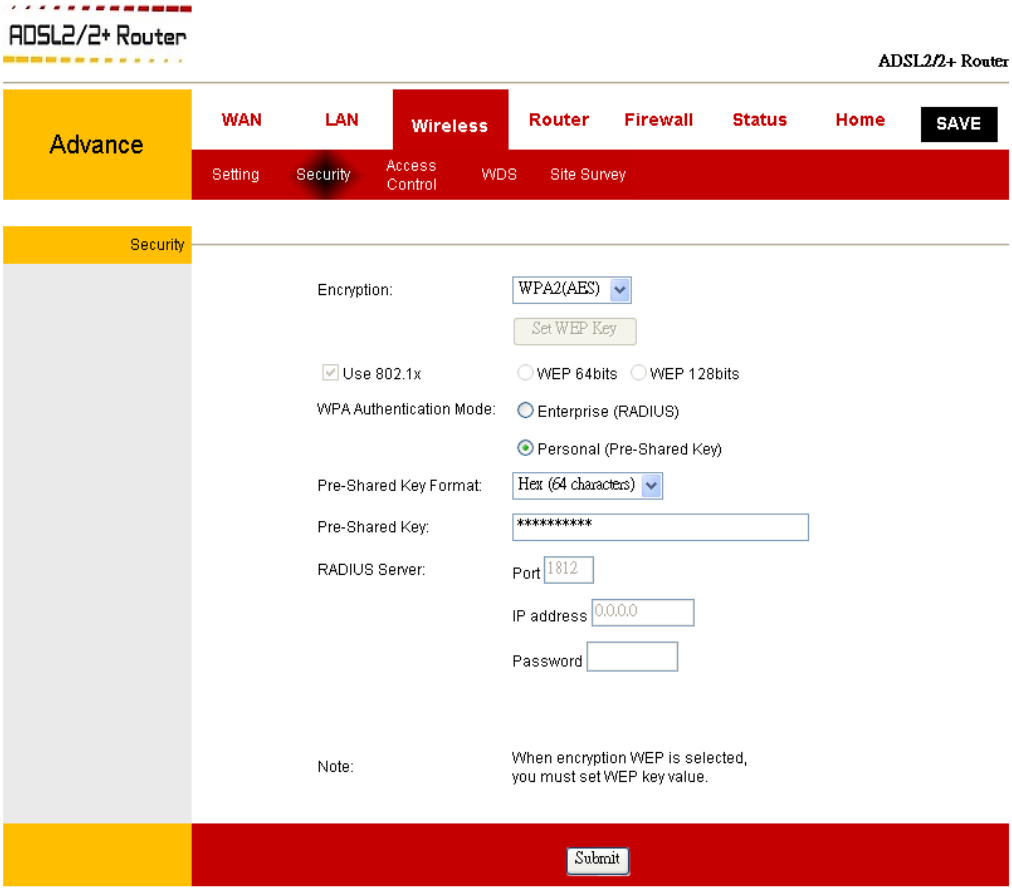
  - **Passphrase:** A **passphrase** is a sequence of words or other text used to control access to a system. A passphrase is similar to a password in usage, but is generally longer for added security. The **PassPharse** can be letters, symbols or numbers. No space can be used in this field.
  - **Hex (64 characters):** The **Hex (64characters)** can be letters, symbols or numbers. No space can be used in this field.

- Click **"Submit"** after setup.
- To make the change permanent, click on **SAVE**.

4.4.3.2.4 Wireless Security – WPA2 (AES)

IEEE 802.11i, also known as **WPA2**, is an amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks. This standard supersedes the previous security specification, Wires Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as **WPA2**.

Figure below shows the default setting of the **Wireless – Security – WPA2 (AES)** page.



- **Use 802.1x: 802.1x** is a security protocol for Wireless Local Area Networks (WLAN). It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on Extensible Authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the RADIUS (Remote Authentication Dial-In User Service) protocol. When **802.1x** is **"Enabled"** by default.

- **WPA Authentication Mode:** Click the radio button to enable **"Enterprise (RADIUS)"** or **"Personal (Pre-Shared Key)"** mode.

  - ☑ **Enterprise (RADIUS) Mode:** When Enterprise (RADIUS) mode is check, the following RADIUS Server's data have to be provided at the same time:

    - ◆ **Port:** The protocol port of the RADIUS server.
    - ◆ **IP address:** The IP address of the RADIUS server. Used for authentication.
    - ◆ **Password:** The Password that the AP shares with the RADIUS server.

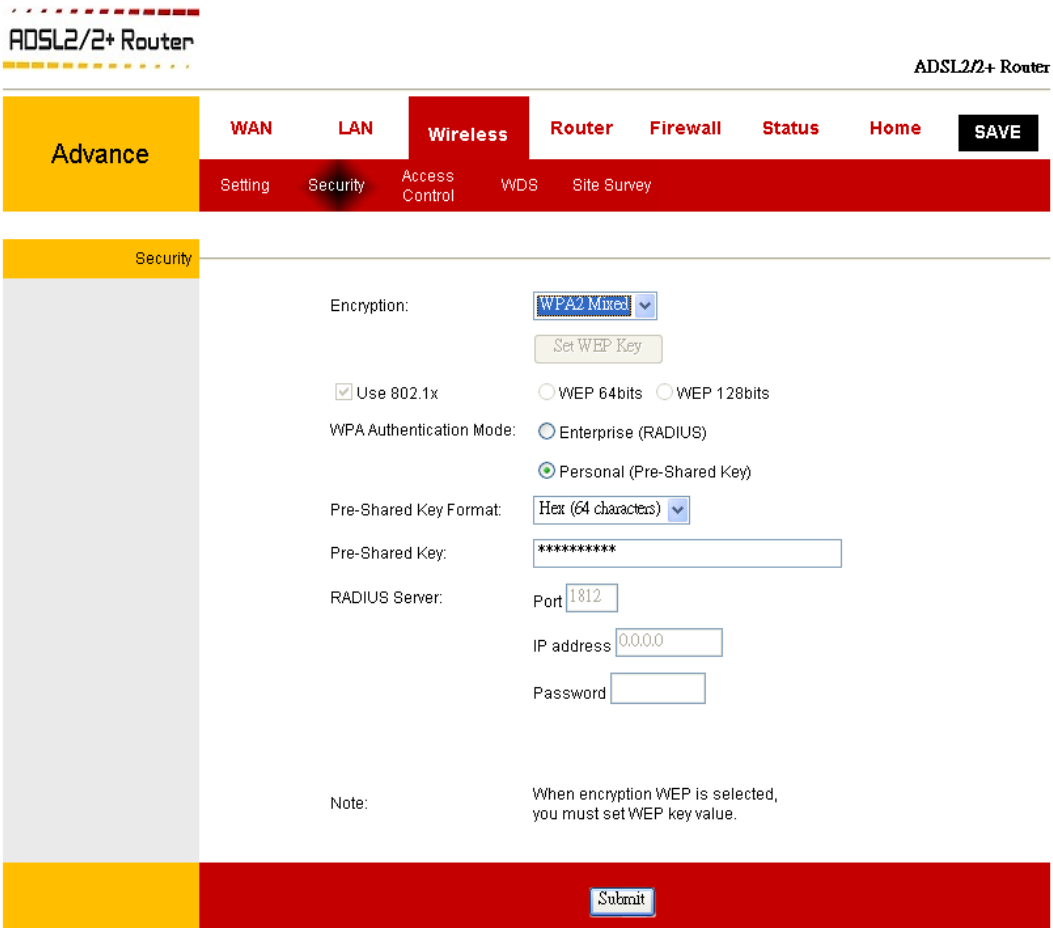
  - ☑ **Personal (Pre-Shared Key) Mode:** A Pre-Shared Key identifies a communication party during the IKE negotiation. It is called **"Pre-Shared"** because you have to share it with another party before you can communicate with them over a secure connection. Click and select your **"Pre-Shared Key Format"**. Two different format are provided:

    - ◆ **Passphrase:** A **passphrase** is a sequence of words or other text used to control access to a system. A passphrase is similar to a password in usage, but is generally longer for added security. The **PassPharse** can be letters, symbols or numbers. No space can be used in this field.
    - ◆ **Hex (64 characters):** The **Hex (64characters)** can be letters, symbols or numbers. No space can be used in this field.

- Click **"Submit"** after setup.
- To make the change permanent, click on **SAVE**.

4.4.3.2.5 Wireless Security – WPA2 (Mixed)

WPA (Mixed) is a more advance security mechanism that support both WPA and WPA2 functionality. Figure below shows the default setting of the **Wireless – Security – WPA2 (Mixed)** page.



- **Use 802.1x: 802.1x** is a security protocol for Wireless Local Area Networks (WLAN). It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on Extensible Authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the RADIUS (Remote Authentication Dial-In User Service) protocol. When **802.1x** is **"Enabled"** by default.

- **WPA Authentication Mode:** Click the radio button to enable **"Enterprise (RADIUS)"** or **"Personal (Pre-Shared Key)"** mode.

  ☑ **Enterprise (RADIUS) Mode:** When Enterprise (RADIUS) mode is check, the following RADIUS Server's data have to be provided at the same time:

  - **Port:** The protocol port of the RADIUS server.
  - **IP address:** The IP address of the RADIUS server. Used for authentication.
  - **Password:** The Password that the AP shares with the RADIUS server.

☑ **Personal (Pre-Shared Key) Mode:** A Pre-Shared Key identifies a communication party during the IKE negotiation. It is called **"Pre-Shared"** because you have to share it with another party before you can communicate with them over a secure connection. Click and select your **"Pre-Shared Key Format"**. Two different format are provided:

- **Passphrase:** A **passphrase** is a sequence of words or other text used to control access to a system. A passphrase is similar to a password in usage, but is generally longer for added security. The **PassPharse** can be letters, symbols or numbers. No space can be used in this field.
- **Hex (64 characters):** The **Hex (64characters)** can be letters, symbols or numbers. No space can be used in this field.

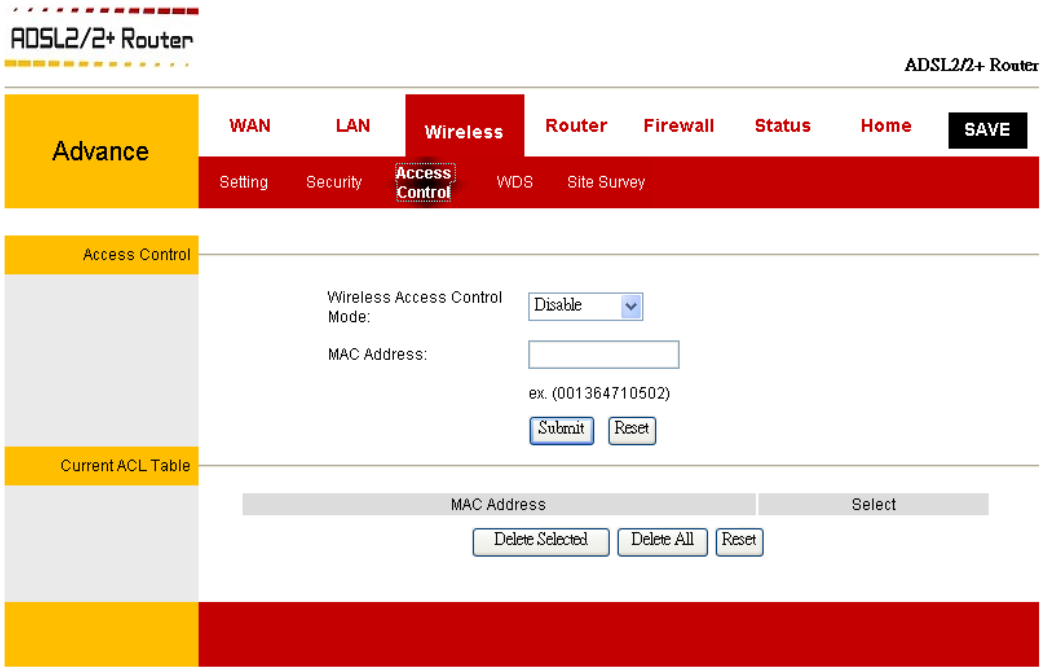
- Click **"Submit"** after setup.
- To make the change permanent, click on **SAVE**.

4.4.3.3 Advance – Wireless – Access Control

Access Control: By default, any wireless computer that is configured with the correct wireless network name or SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses. Only the valid MAC address that has been configured can access the wireless LAN interface.

Note: To enable the Access Control functionality, this 4 Ports 11g Wireless ADSL2/2+ Router have to set to **"AP"** mode. Go to or refer to **Advance – Wireless – Setting** for the setting detail.

You can create an **"Allow"** or **"Deny"** access list from the Access Control List screen by performing the following procedures describe in next section. By clicking the **Advance – Wireless – Access Control**, the following web page appear:



- **Wireless Access Control Mode:** Select **"Disable"**, **"Allow Listed"** or **"Deny Listed"** from the drop down manual.

- **MAC Address:** Enter the MAC Address of the wireless network that are Allow or Deny to access your 4 Ports 11g Wireless ADSL2/2+ Router. Then click **Submit** to include to your Access List.

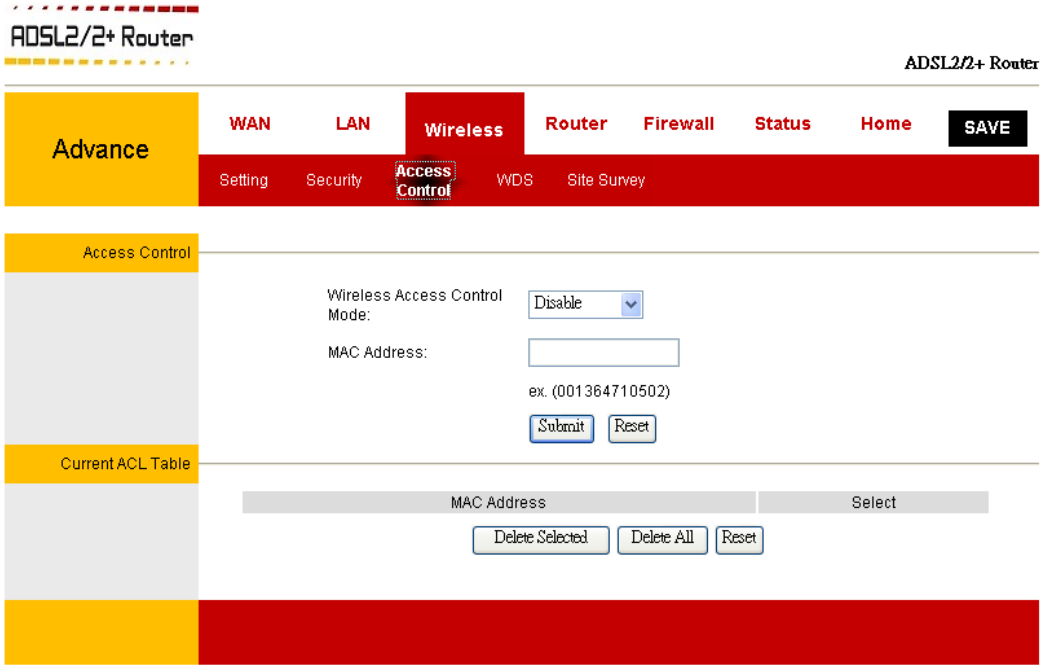
- **Submit:** Click **Submit** to complete and confirm your setting.

- **Reset:** Click **Reset** to ignore or clear all the changes.

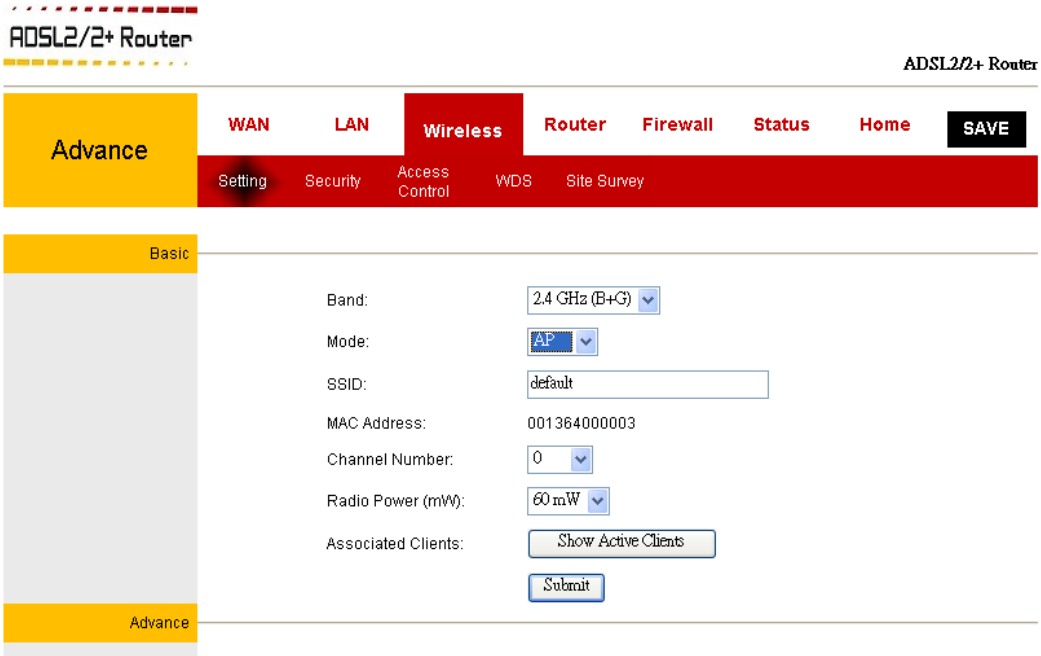
- To complete and save the setting, click **SAVE** button.

4.4.3.3.1 Setting Up Access Control List

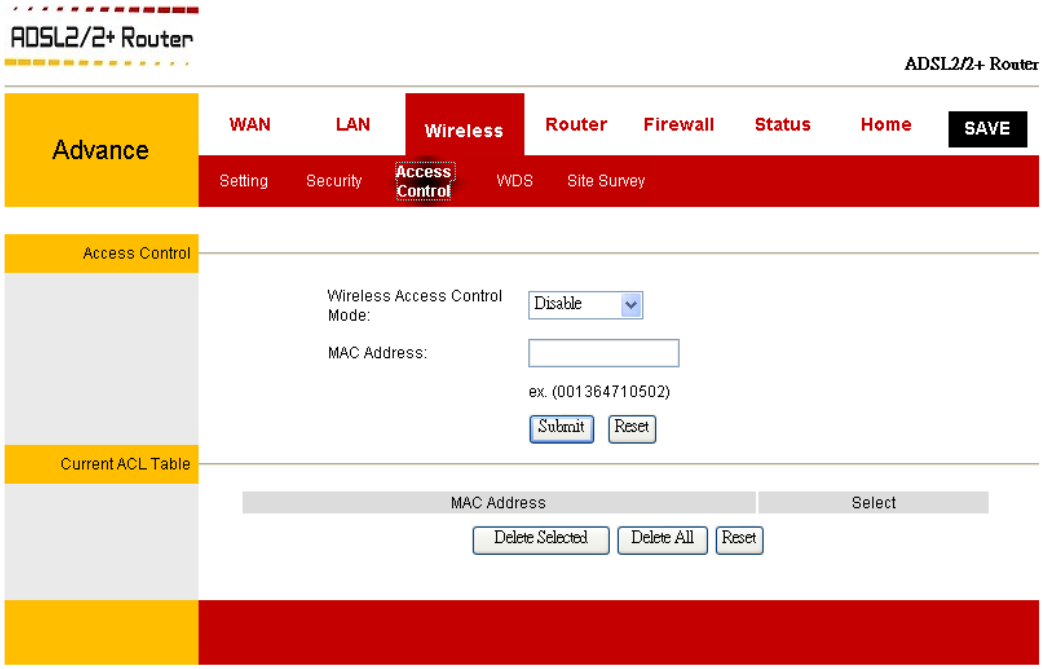
Click on **Advance – Wireless – Access Control** tab, the following default screen display. Follow the following procedures to setup your Access Control Table.



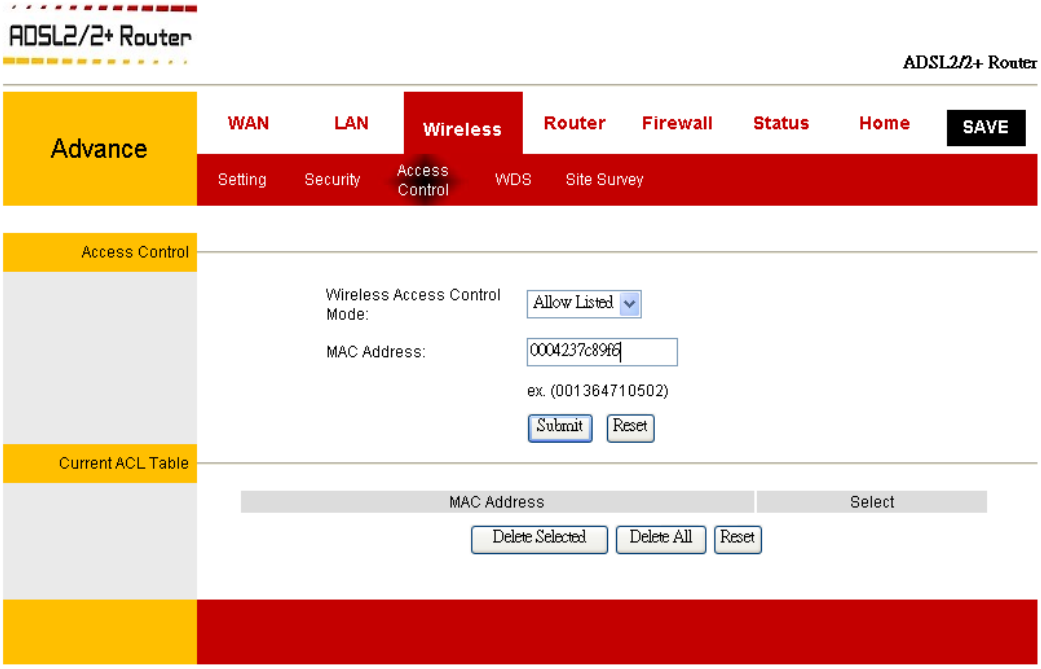
1. Go to Wireless – Setting, set this 4 Ports 11g Wireless ADSL2/2+ Router to **"AP"** mode. Click **"Submit"** after setup. A **"Change setting successfully"** wizard will display. Click **"OK"** and return to the **Wireless – Setting** page.



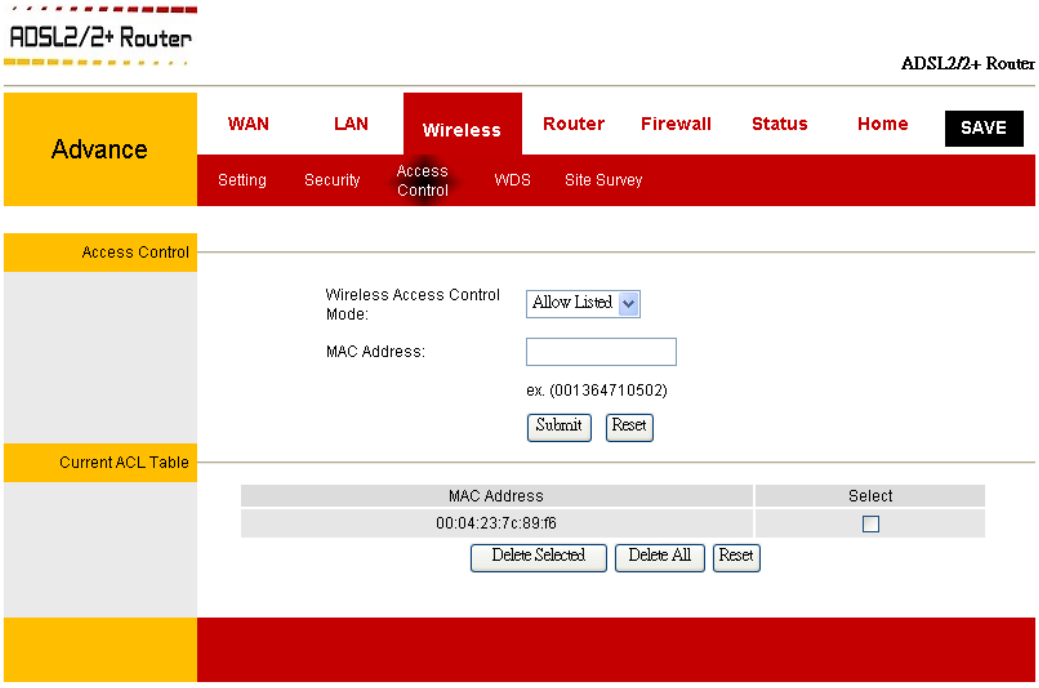
2. Click the **Wireless – Access Control** tab. The following screen display.



3. Select **Wireless Access Control Mode** from the drop down manual. Three different mode are available: **"Disable"**, **"Allow List"** and **"Deny List"**.
4. Enter the **MAC Address** you are going to **"Allow"** or **"Deny"**. Click **"Submit"** after setup. This example shows the **"Allow Listed"** with **MAC Address: 00:04:23:7c:89:f6**.



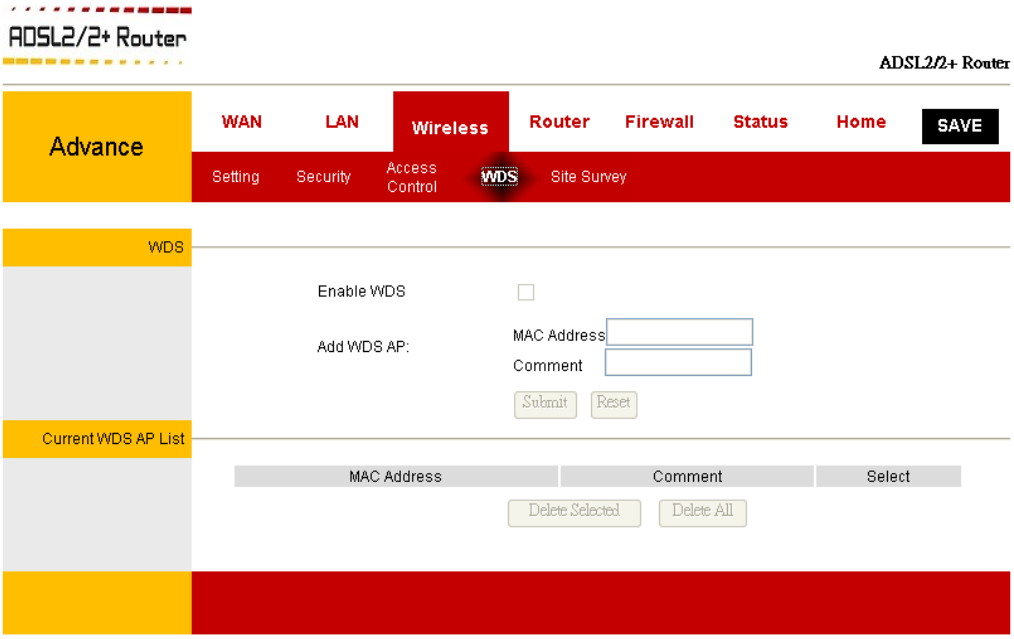
5. A **“Change setting successfully”** wizard will display. Click **“OK”** and return to the **Wireless – Access Control** setting page. The following screen display. The **Current ACL Table** will show the MAC Address list you’d created.



4.4.3.4 Advance – Wireless – WDS

Wireless Distribution System (**WDS**) is a system that interconnects BSS to build a premise wide network. WDS network allows users of mobile equipment to roam and stay connected to the available network resources. You can configure your 4 Ports 11g Wireless ADSL2/2+ Router as **WDS** mode using the **Wireless – WDS** page. Click the **Wireless – WDS** button, the following configuration home page display.

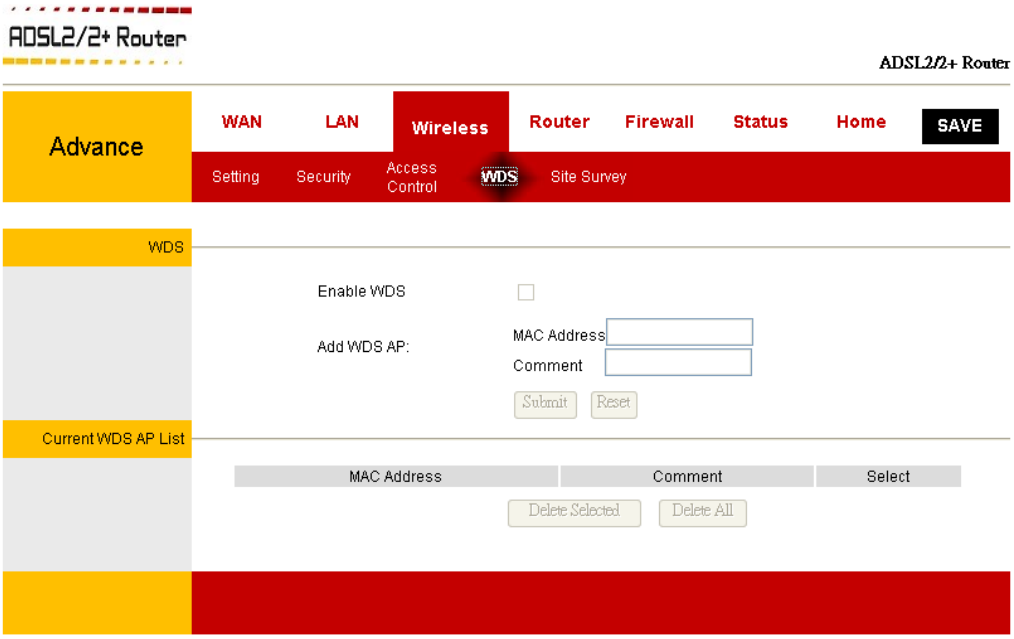
Note: To enable the **WDS** functionality, you have to set your wireless mode to WDS mode. Click **Wireless – Setting** to change your wireless mode.



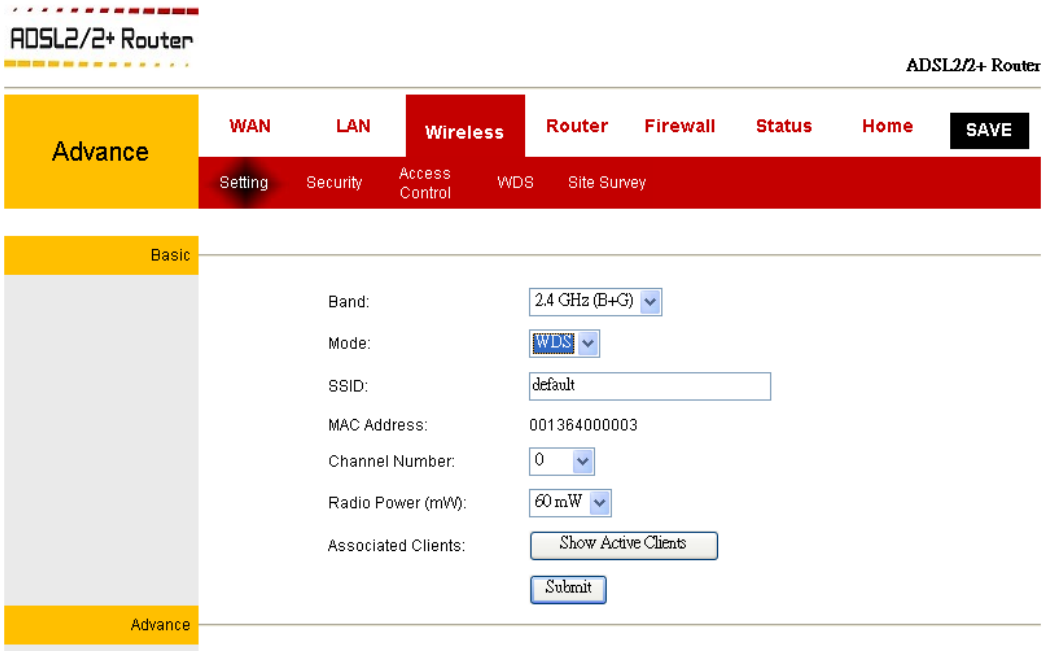
- **Enable WDS:** Click to enable WDS Mode.
- **Mac Address:** The associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.
- **Comment:** The WDS name used to identify WDS network.
- **Submit:** Click **Submit** to complete and confirm your setting.
- **Reset:** Click **Reset** to ignore or clear all the changes.
- To complete and save the setting, click **SAVE** button.

4.4.3.4.1 Setting Up WDS AP List

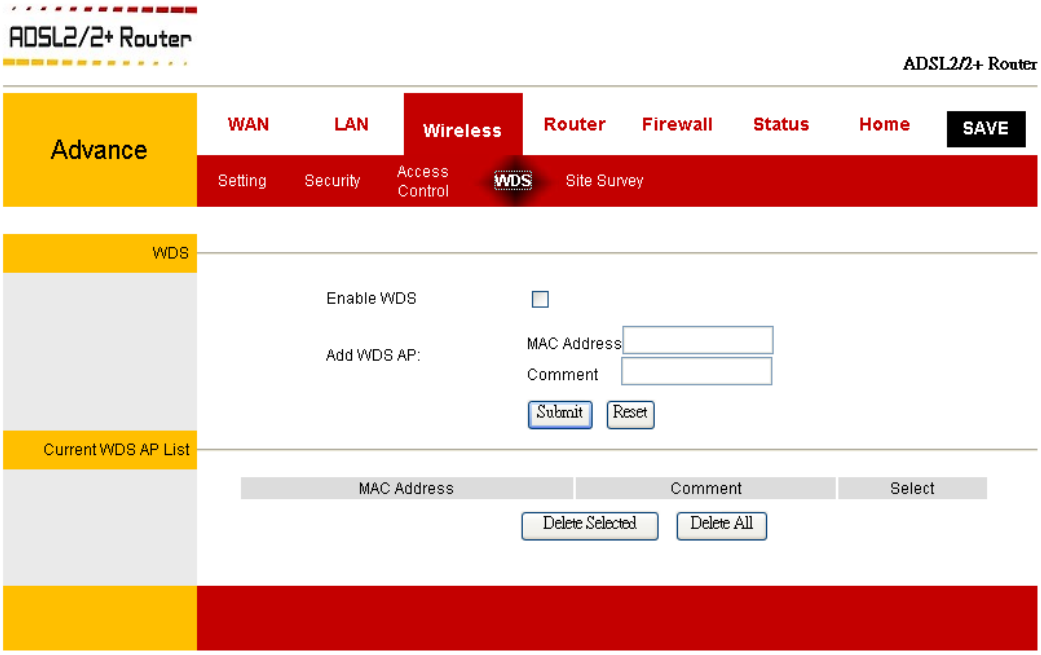
Click on **Advance – Wireless – WDS** tab, the following default screen display. Follow the following procedures to setup your WDS AP List.



1. Go to **Wireless – Setting**, set this 4 Ports 11g Wireless ADSL2/2+ Router to **"WDS"** mode. Click **"Submit"** after setup. A **"Change setting successfully"** wizard will display. Click **"OK"** and return to the **Wireless – Setting** page.

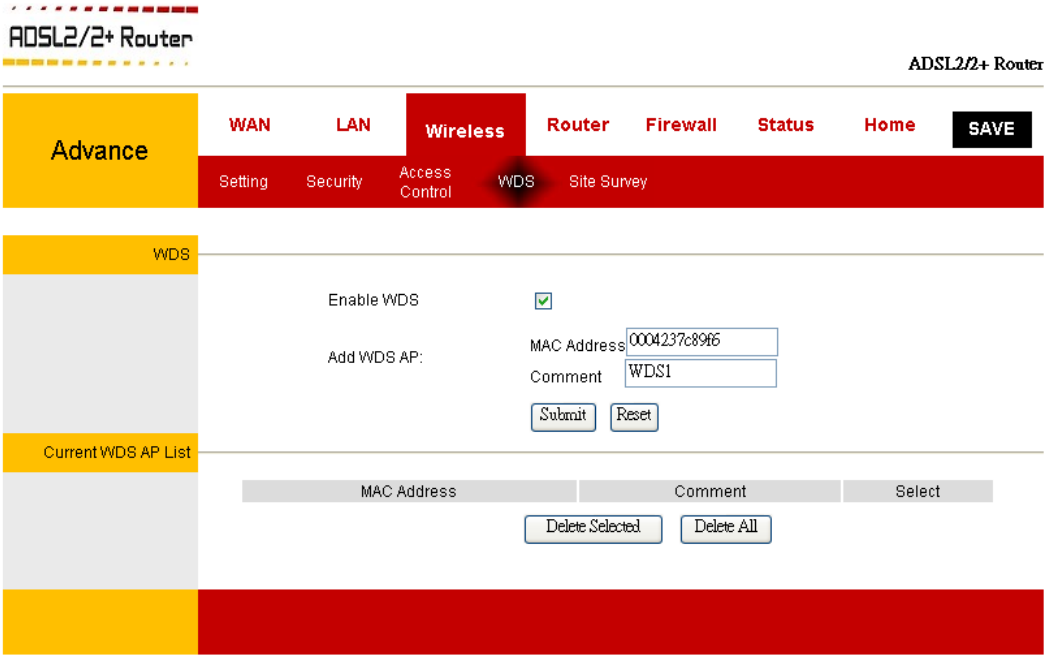


2. Click the **Wireless – WDS** tab. The following screen display.

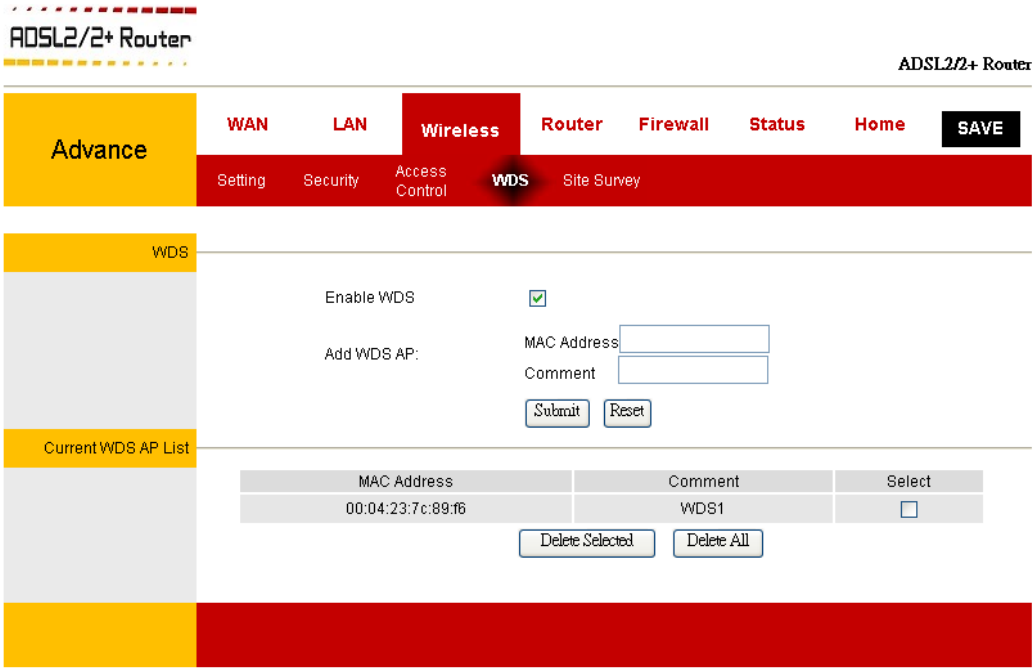


3. Check to enable **WDS** mode.

4. Enter the WDS AP **MAC Address** and WDS name (Comment) used to identify WDS network. Click **"Submit"** after setup. This example shows with **MAC Address: 00:04:23:7c:89:f6** and **Comment: WDS1**

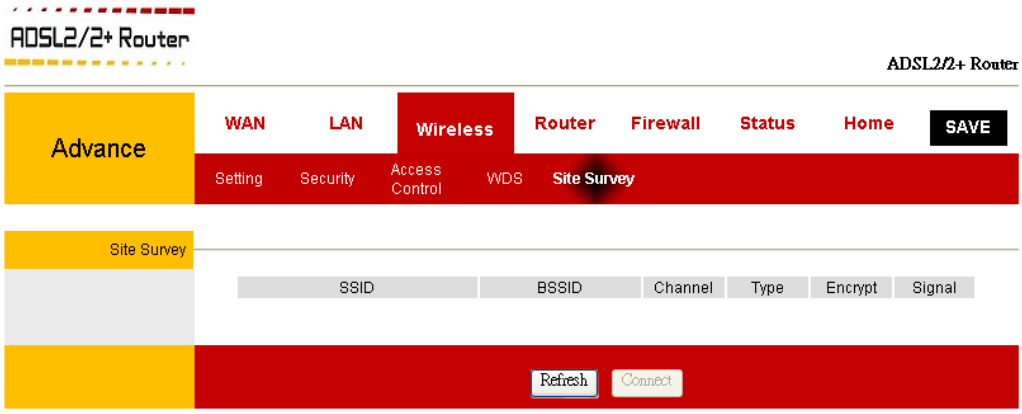


5. A **“Change setting successfully”** wizard will display. Click **“OK”** and return to the **Wireless – WDS** setting page. The following screen display. The **Current WDS AP List** will show the MAC Address list and WDS name (Comment) you’d created.

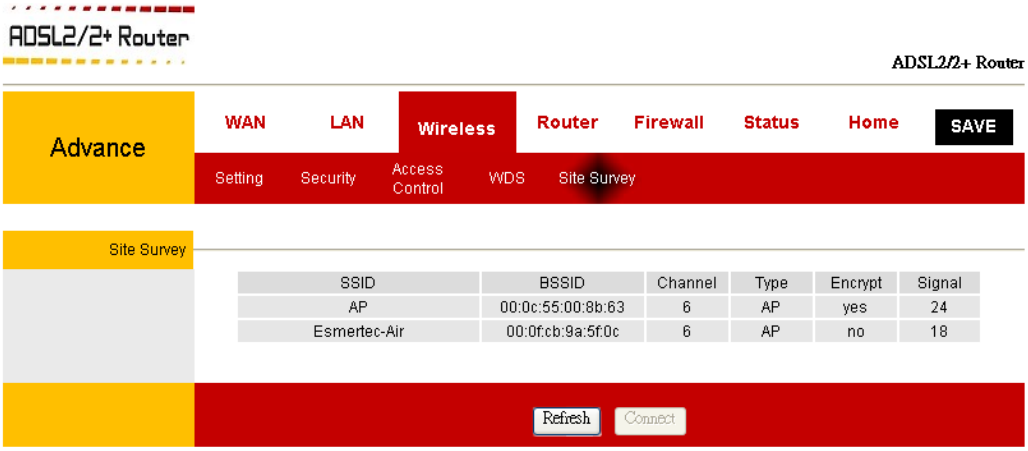


4.4.3.5 Advance – Wireless – Site Survey

The **Site Survey** is a useful utility that help to scan nearby Wireless AP station. Click on **Advance – Wireless – Site Survey** tab, the following default screen display.



Click the **Refresh** button, the following screen display:

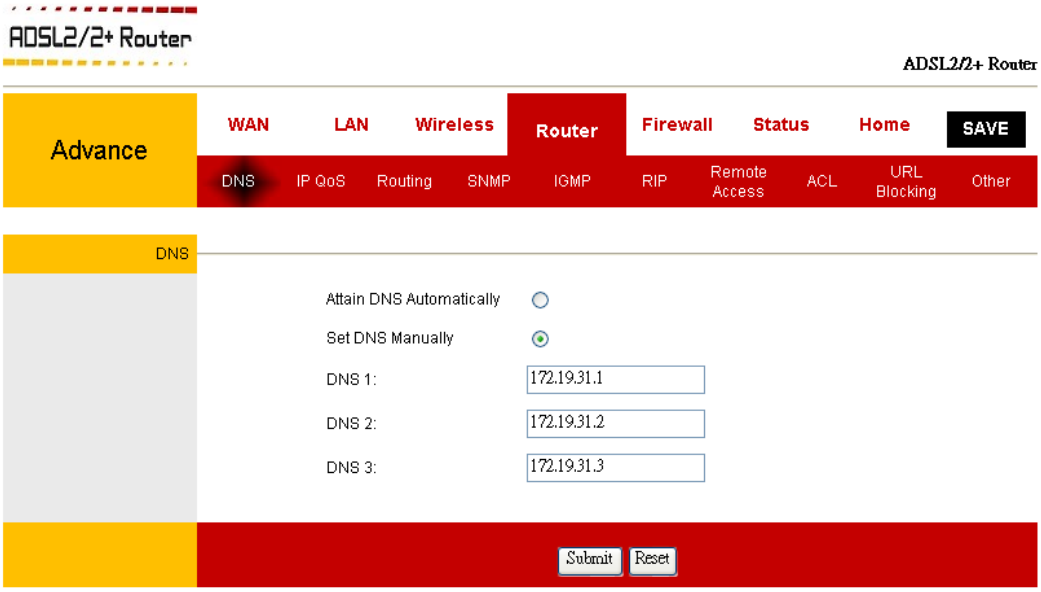


- **SSID:** The Service Set Identifier (SSID) of the scanned wireless network.
- **BSSID:** Basic Service Set Identifier. The unique identifier for an access point in a BSS network. The Wireless LAN specification defines a BSSID as the MAC Address of the station in an Access Point (AP) in a BSS infrastructure mode.
- **Channel:** The appropriate channel of the scanned wireless network. All access points and wireless PC adaptors must share the same channel to interoperate.
- **Type:** The scanned Wireless station type.
- **Encrypt:** Authentication needed to access the Wireless AP.
- **Signal:** Wireless AP signal strength.
- **Refresh:** Click Refresh to reload the Site Survey page.

4.4.4 Advanced – Router

The **Advance – Router** configuration homepage provides access to advanced networking, management and routing capabilities. Click the **Advanced – Router** tab and the following screen will pop-up.

The **Advance – Router** section allows you to perform advanced configuration functions for existing connections including DNS, IP QoS, Routing, SNMP, IGMP, RIP, Remote Access, ACL and URL Blocking.



4.4.4.1 Advanced – Router – DNS

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (e.g., “Google.com”) to the equivalent numerical IP addresses that are used for Internet routing.

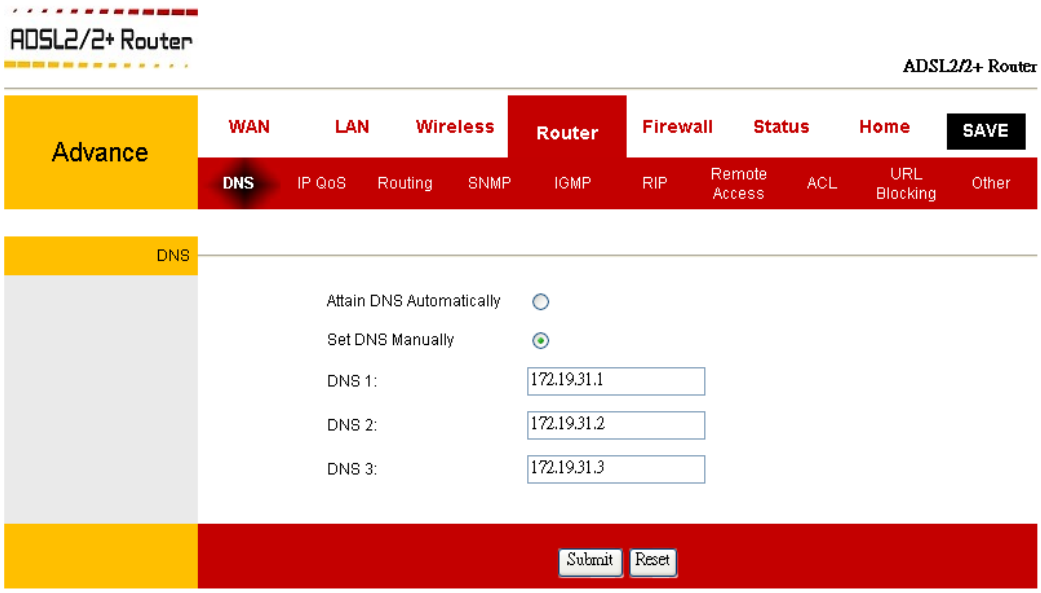
When a PC user types a domain name into a browser, the PC must first send a request to a DNS server to obtain the equivalent IP address. The DNS server will attempt to look up the domain name in its own database, and will communicate with higher-level DNS servers when the name cannot be found locally. When the address is found, it is sent back to the requesting PC and is referenced in IP packets for the remainder of the communication.

Multiple DNS addresses are useful to provide alternatives when one of the servers is down or is encountering heavy traffic. ISPs typically provide primary and secondary DNS addresses, and may provide additional addresses. Your LAN PCs learn these DNS addresses in one of the following ways:

- **Statically:** If your ISP provides you with their DNS server addresses, you can assign the addresses to each PC by modifying the PCs' IP properties.
- **Dynamically from a DHCP pool:** You can configure the DHCP Server feature under the **Advance – LAN – LAN** configuration page.

In either case, you can specify the actual addresses of the ISP's DNS servers (on the PC or in the DHCP pool), or you can specify the address of the LAN interface on the 4 Ports 11g Wireless ADSL2/2+ Router (e.g., 192.168.1.1). When you specify the LAN port IP address, the device performs DNS relay, as described in the **Advance – LAN – LAN** section.

Click the **Advance – Router** tab, and then click **DNS** in the task bar, the **DNS Configuration** page displays.



- **Attain DNS Automatically:** Check if you would like to attain DNS automatically.

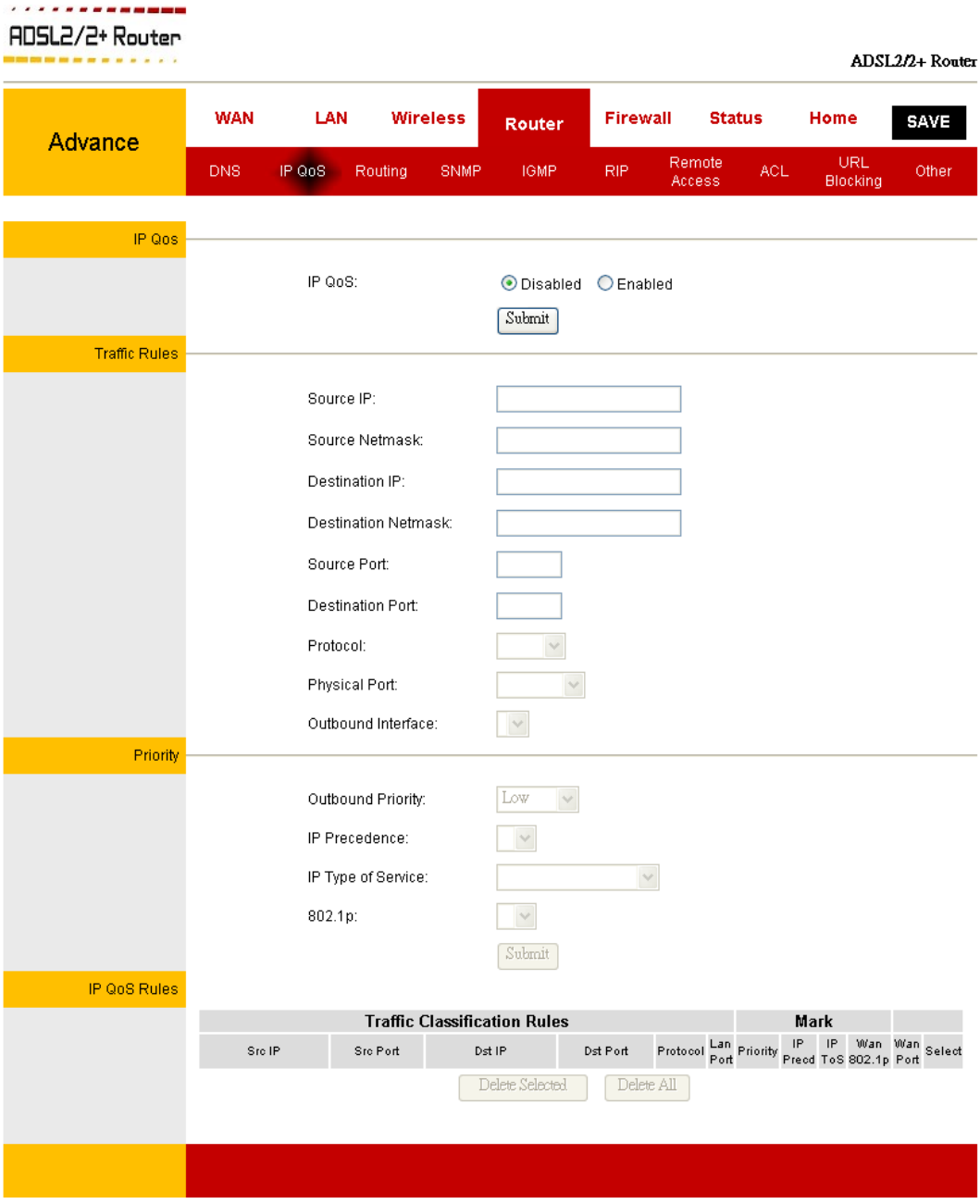
- **Set DNS Manually:** Set the DNS Address manually. The DNS data will be provided by your ADSL service provider.

- **Submit:** Click Submit to confirm your setting.

- **Reset:** Click Reset to give up all your current setting.

4.4.4.2 Advanced – Router – IP QoS

Quality of service (QoS) is an important feature for this release. The QoS framework allows network administrators to configure the routers to meet the real time requirements for voice and video. When QoS is enabled, the designated machine, application or person would have precedence over peers when competing for bandwidth. The IP QoS Setup page allows you to configure QoS for a connection, view previously configured QoS rules, add a new rule, or delete an existing rule.



Refer to next page on the description of the IP QoS Screen settings.

■ IP QoS:

- ☑ **IP QoS:** Click **Enabled** or **Disabled** the IP QoS functionality.
- ☑ **Submit:** Click **Submit** to confirm your setting.

■ Traffic Rules:

- ☑ **Source IP:** The IP address of the traffic source.
- ☑ **Source Netmask:** The Netmask of the source.
- ☑ **Destination IP:** The IP address of the traffic destination.
- ☑ **Destination Netmask:** The Netmask of the destination.
- ☑ **Source Port:** The port of the source.
- ☑ **Destination Port:** The port of the destination.
- ☑ **Protocol:** The selections are TCP, UDP and ICMP.
- ☑ **Physical Port:** The selections are Port 1 through Port 4.
- ☑ **Outbound Interface:** The Outbound Interface is the interface which allows you to filter outbound (from the user side LAN to the WAN) packets.

■ Priority:

- ☑ **Outbound Priority:** There are 3 Outbound Priority available : Low, Medium and High.
- ☑ **IP Precedence:** Select the IP Precedence from 0 ~ 7.
- ☑ **IP Type of Service:** The IP Type of Service field allows you to assign a service to this traffic. The values for the IP Type of Service can be: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput and Minimize Delay.
- ☑ **802.1p:** An IEEE standard for providing Quality of Service (QoS) in 802-based networks. 802.1p uses three bits (defined in 802.1q) to allow switches to reorder packets based on priority level.
- ☑ **Submit:** Click **Submit** to confirm your setting.

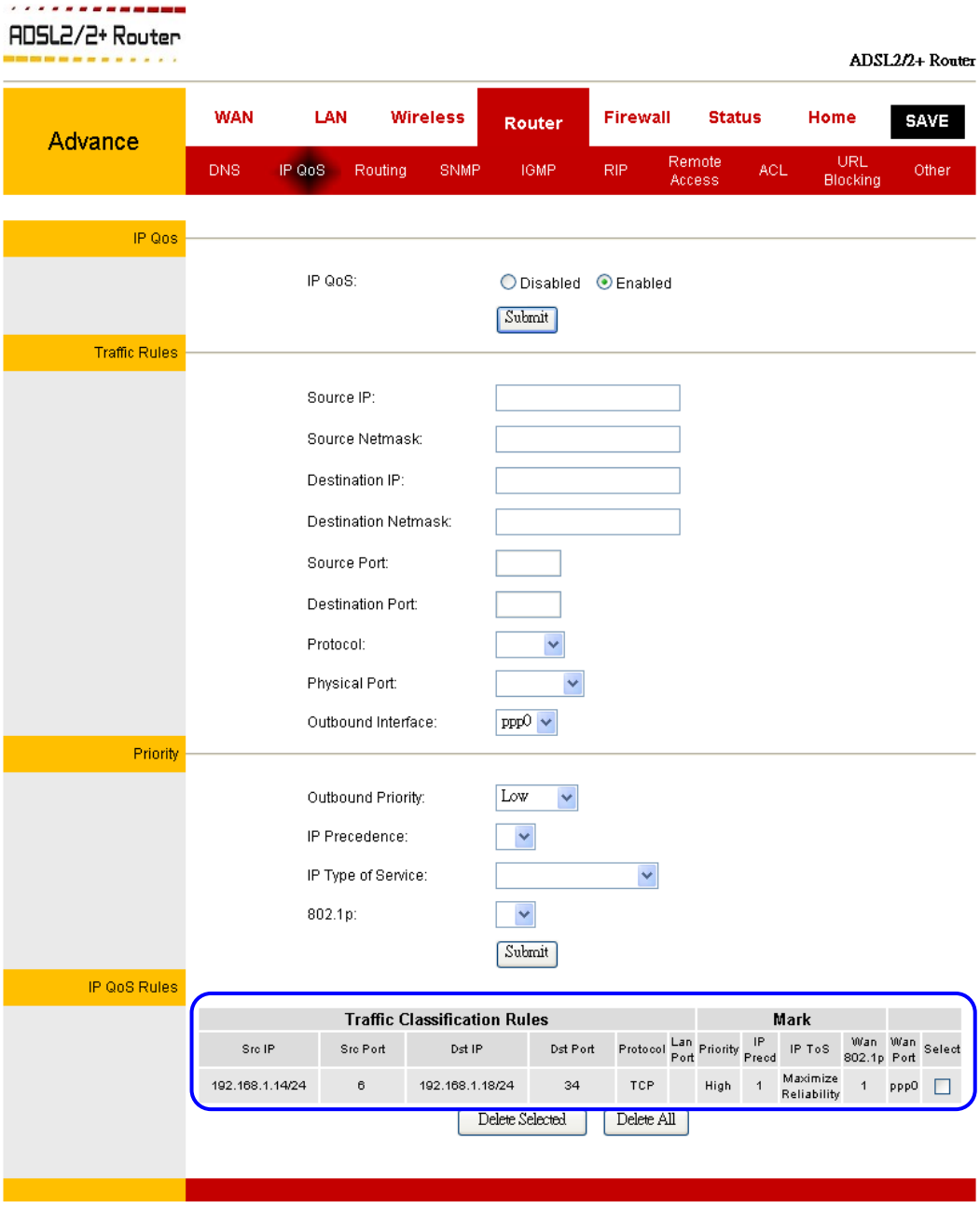
■ IP QoS Rule:

- ☑ **IP QoS Rule:** The IP QoS Rule's table.

4.4.4.2.1 IP QoS Rule Setup

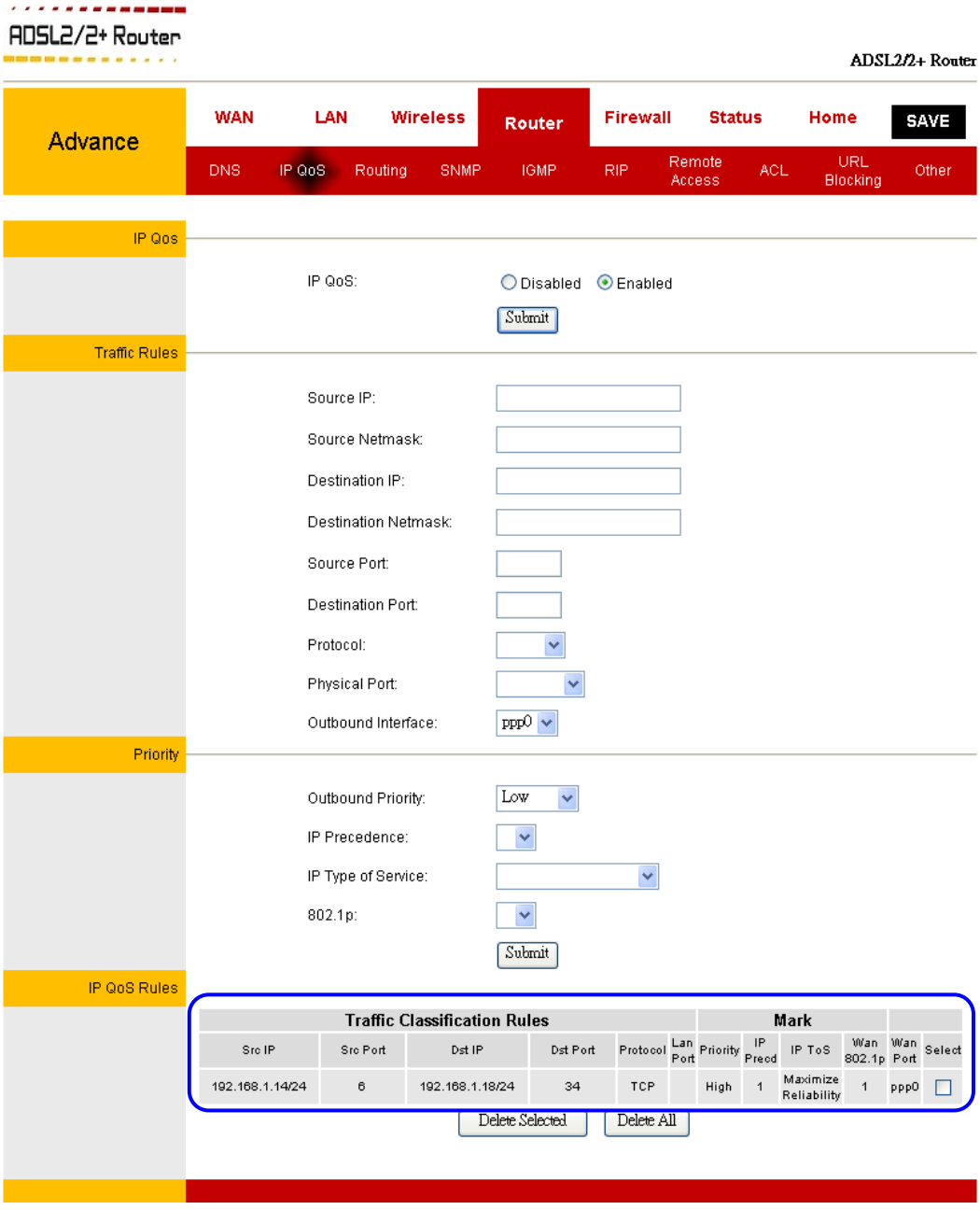
The IP QoS Rule Setup page allows you to define a traffic rule for a specified connection. Use the following procedures to access the IP QoS Rule Setup Page.

1. From the **IP QoS** setup page, **c**heck **Enable IP QoS**.
2. Click **Submit** to confirm your setting. A **"Change setting successfully!"** screen display. Click **"OK"** and get back to the **IP QoS** setting page.
3. Use Section 4.4.4.2 as a reference, and enter the required fields on the IP QoS Setup page
4. Click **Submit** to temporarily save the setting.
5. To make the change permanent , click on the **SAVE** tab.
6. The IP QoS Rule has been created as illustrated in figure below:



4.4.4.2.2 Delete An IP QoS Rule

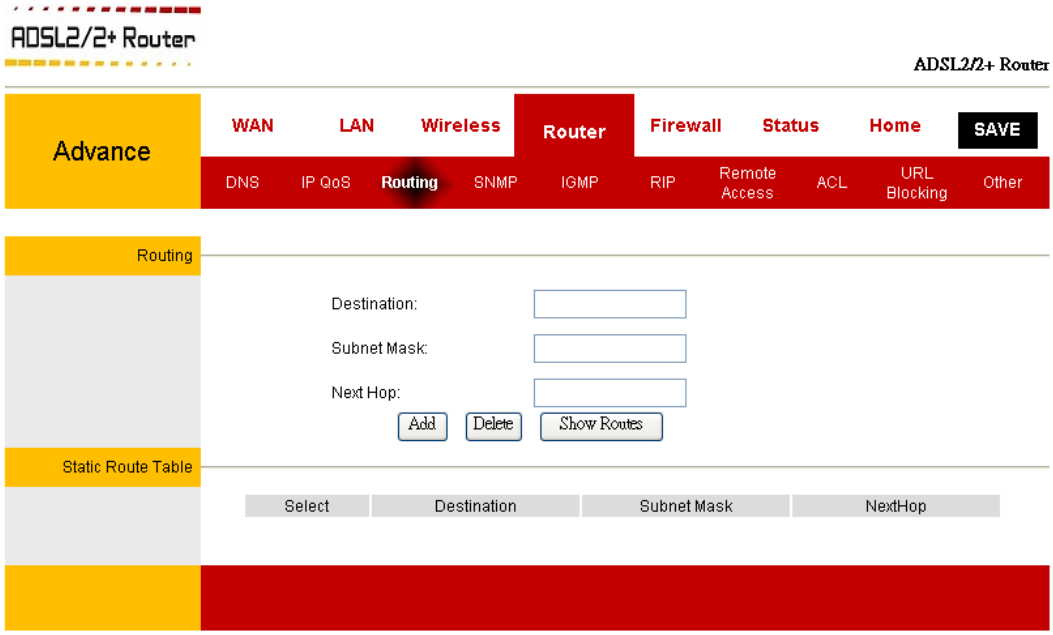
The IP QoS Rule has been created as illustrated in figure below. Use the following procedures to delete an existing IP QoS Rule.



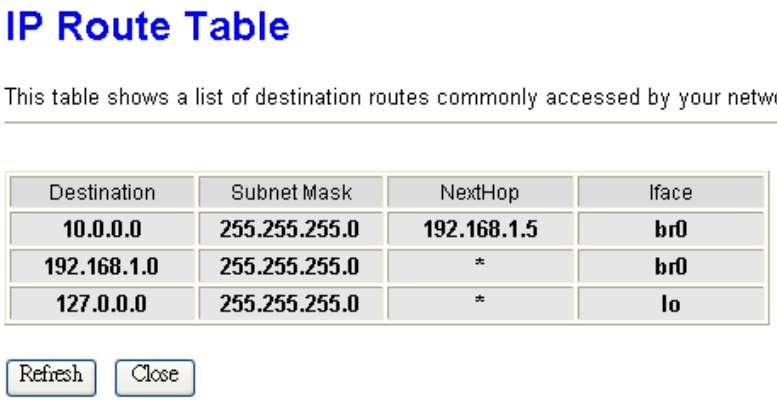
1. Check **Select** next to the traffic rule you want to delete.
2. Click **"Delete Selected"**.
3. To make the change permanent, click on the **SAVE** tab.

4.4.4.3 Advanced – Router – Routing

If the router is required to serve more than one network, you will need to set up a **Static Route** between the networks. Static routing can be used to allow users from one IP domain to access the Internet through the Router in another domain. A Static Route provides the defined pathway that network information must travel to reach the specific host or network which is providing Internet access.



- **Destination:** The network IP address of the subnet. (You can also enter the IP address of each individual station in the subnet).
- **Subnet Mask:** The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion.
- **Next Hop:** The Next Hop IP Address. It defines the IP Address between network nodes that data packets will travel.
- **Add:** Click **Add** tab to add in new Routing list.
- **Delete:** Click **Delete** tab to delete the Static Route from the table.
- **Show Routes:** Click **Show Routes** tab and the following screen display:

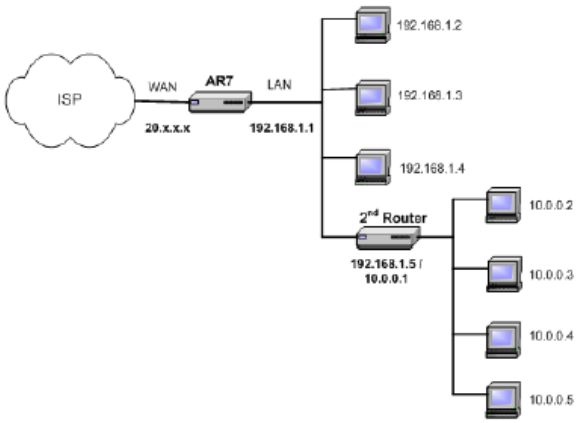


☑ **Refresh:** Click **Refresh** to reload the current page.

☑ **Close:** Click **Close** to close the IP Route Table.

4.4.4.3.1 Static Routing Configuration Procedure

Suppose you have a network like the one shown in below. In your LAN, you have a 4 Ports 11g Wireless ADSL2/2+ Router (192.168.1.1) and three stations connected to it (192.168.1.x). A subnet is added to your LAN group by adding a second router (192.168.1.5/10.0.0.1) with four stations (10.0.0.x) connected to it. The four stations in the subnet cannot receive packets unless they are added to the routing table of your 4 Ports 11g Wireless ADSL2/2+ Router. You can add each individual station to the routing table using the **Routing** page, or more easily, you can add the whole subnet in one entry. Section 4.4.8.2 explains how to add the subnet to the 4 Ports 11g Wireless ADSL2/2+ Router routing table.

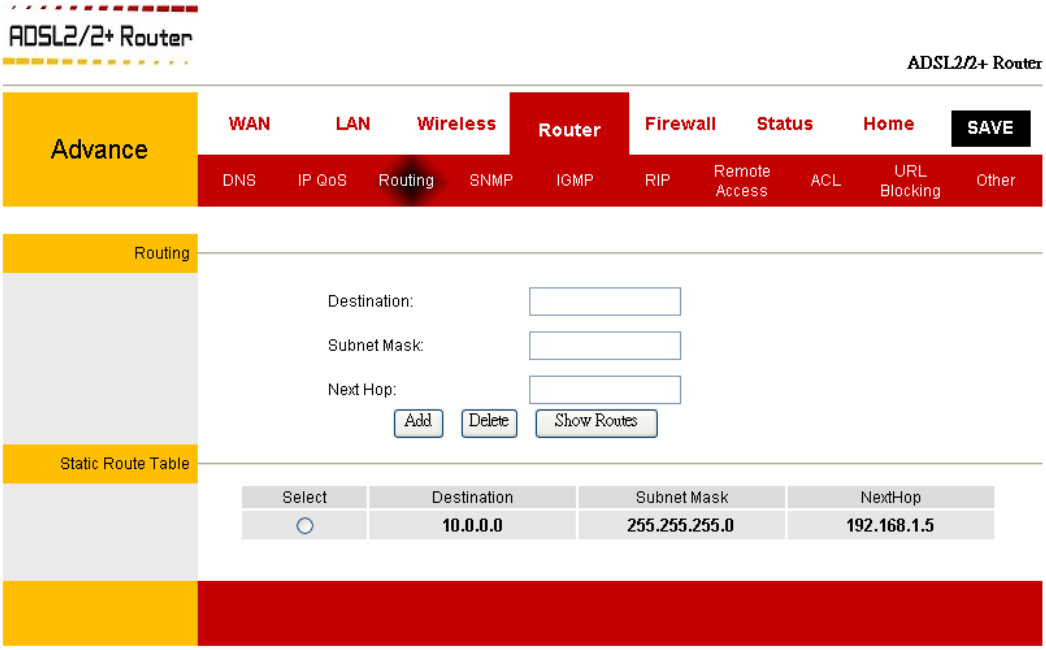


1. Enter or leave the default entry for the following parameters:

   - ☑ **New Destination IP**: 10.0.0.0 (the network IP address of the subnet)
   - ☑ **Mask**: 255.255.255.0 (the subnet mask)
   - ☑ **Next Hop**: 192.168.1.5 (the LAN-side IP address of the second router, through which the stations in the subnet access the network)

   You are telling the 4 Ports 11g Wireless ADSL2/2+ Router that a new subnet with an IP of *10.0.0.0* and a Netmask of *255.255.255.0* has been added and can access the 4 Ports 11g Wireless ADSL2/2+ Router via station *192.168.1.5*.

2. Click **Add** to temporarily save the settings. You have added the subnet to the routing table (Figure below). You have added the subnet to the routing table (Figure below). The four stations in the subnet can receive packets from the WAN.



Note: You can add up to 16 entries. You can also delete any entry using the **Select** checkbox.

3. Click **SAVE** again when you finish making all the changes.

Note: The changes take effect when you click **Add**; however, if the 4 Ports 11g Wireless ADSL2/2+ Router configuration is not saved, these changes will be lost upon 4 Ports 11g Wireless ADSL2/2+ Router reboot.

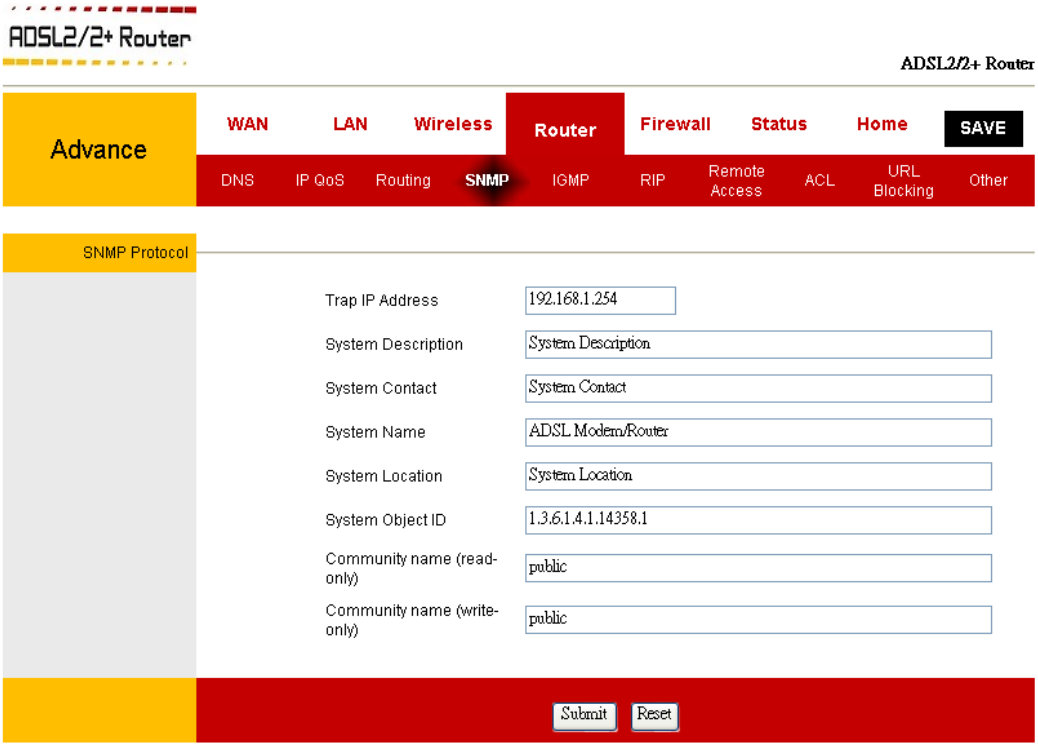
4. To make the change permanent, click **SAVE**.

4.4.4.4 Advance – Router – SNMP

Simple Network Management Protocol (**SNMP**) is an application layer protocol that is used for managing networks. There are several components that make up the SNMP structure, including agents, network management stations (NMS), network management protocols, and a management information base (MIB).

An SNMP agent is a node that resides on the network, typically a computer or a router. The SNMP agent is controlled and configured by the NMS by sending SNMP messages between one another. SNMP agents are logged and identified in a Management Information Base (MIB), in which they are identified by an object identifier (OID).

Click the **Advance – Router – SNMP** tab, the following screen display.



- **Trap IP Address:** This is the IP address to which SNMP traps are sent.
- **SNMP System Identification:** The System Description, System Contact, System Name, System Location, and System OID are provided to identify the SNMP NMS. The System OID is the ID number placed in all Trap reports. Default value for System OID is 1.3.6.1.4.1.4900.
- **Community name (read-only):** This is the password to access public information. The Read Community can be up to 127 characters. Default is **"public"**.
- **Community name (write-only):** This is the password to access private information. The Write Community can be up to 127 characters. Default is **"public"**.
- **Submit:** Click **Submit** to complete the setting.
- **Reset:** Click **Reset** to ignore all the changes.
- To complete and save the setting, click **SAVE** after clicking the **Submit** button.

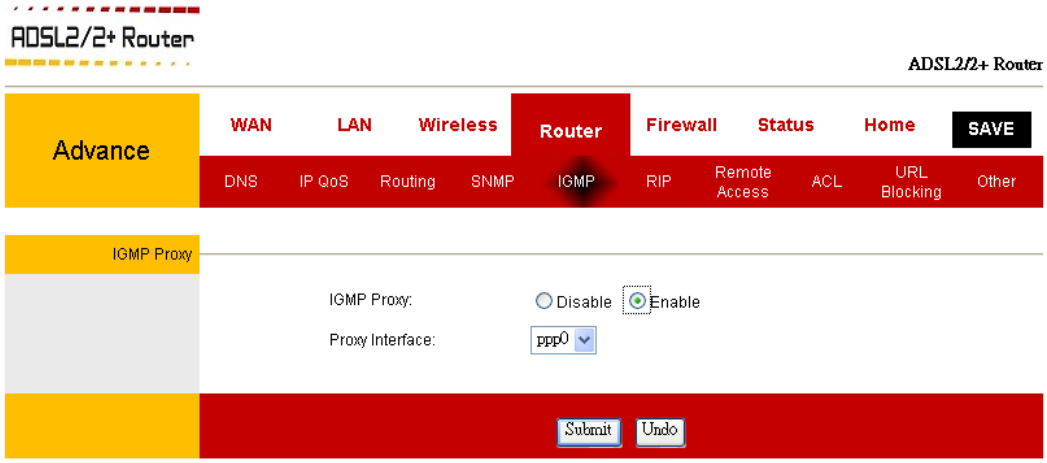
4.4.4.5 Advance – Router – IGMP

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a **Host Group**. A host group is a set of one or more hosts identified by a single IP destination address. The following statements apply to host groups:

- ☑ Anyone can join or leave a host group at will.
- ☑ There are no restrictions on a host's location.
- ☑ There are no restrictions on the number of members that may belong to a host group.
- ☑ A host may belong to multiple host groups.
- ☑ Non-group members may send UDP datagrams to the host group.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers.

IP hosts use Internet group management protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your 4 Ports 11g Wireless ADSL2/2+ Router supports IGMP proxy that handles IGMP messages. When enabled, your 4 Ports 11g Wireless ADSL2/2+ Router acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side.



4.4.4.6 Advance – Router – RIP

Your 4 Ports 11g Wireless ADSL2/2+ Router can be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. Routing devices communicate this information using a variety of IP protocols. This topic describes how to configure your 4 Ports 11g Wireless ADSL2/2+ Router to use one of these, called the Routing Information Protocol (**RIP**).

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected via the ADSL line. Generally, **RIP** is used to enable communication on autonomous networks. An autonomous network is one in which all the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

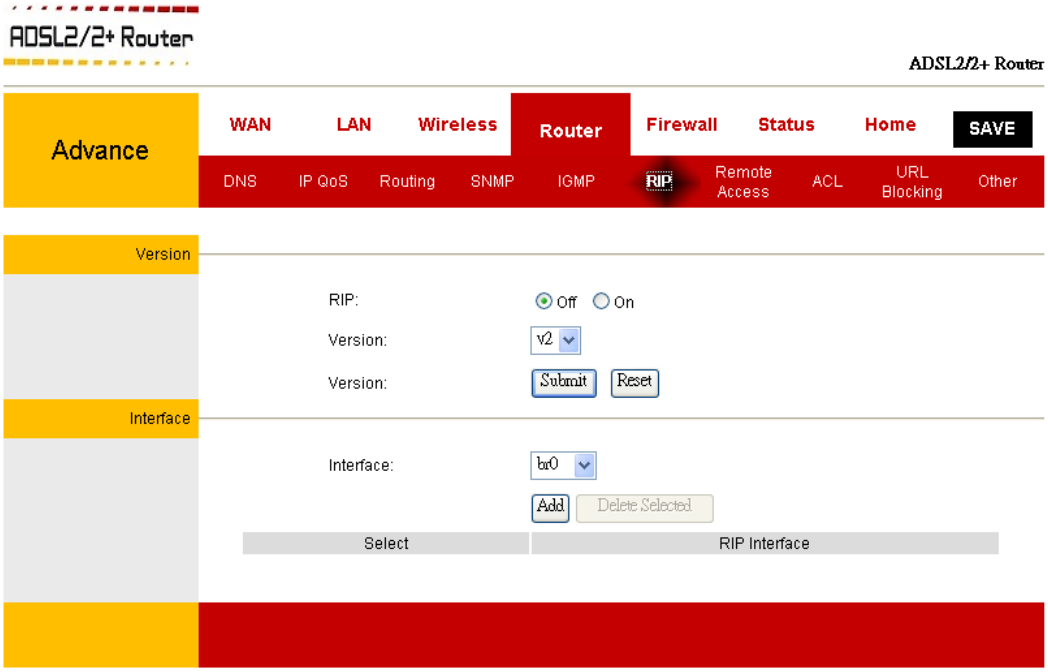
Using **RIP**, each device sends its routing table to its closest neighbor every 30 seconds. The neighboring device in turn passes the information on to its next neighbor and so on until all devices in the autonomous network have the same set of routes.

Most small home or office networks do not need to use **RIP**; they have only one router and one path to an ISP. In these cases, there is no need to share routes, because all routes from the network go to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the 4 Ports 11g Wireless ADSL2/2+ Router). The 4 Ports 11g Wireless ADSL2/2+ Router and your second router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for the networks at the two sites to share the routes used internally within each LAN, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

Click the **Router – RIP** tab, the **RIP** Configuration page will pop-up as shown below. The page contains radio buttons for enabling or disabling the RIP feature and a table listing interfaces on which the protocol is currently running.



- **RIP:** This field allows you to **ON** or **OFF** the RIP session. The resulting RIP session will monitor all network interfaces that are currently available for messages from other RIP routers. RIP is **"Off"** by default.

- **Version:** The following two RIP versions are available:
  - ☑ **v1:** RIP version 1 is the original RIP protocol. Select RIP v1 if you have devices that communicate with this interface that understand RIP version 1 only.
  - ☑ **v2:** RIP version 2 is the preferred selection because it supports "Classless" IP addresses (which are used to create subnets) and other features. Select RIP v2 if all other routing devices on your LAN support this version of the protocol.

- **Submit:** Click **Submit** to complete the setting.
- **Reset:** Click **Reset** to ignore all the changes.
- To complete and save the setting, click **SAVE** after clicking the **Submit** button.

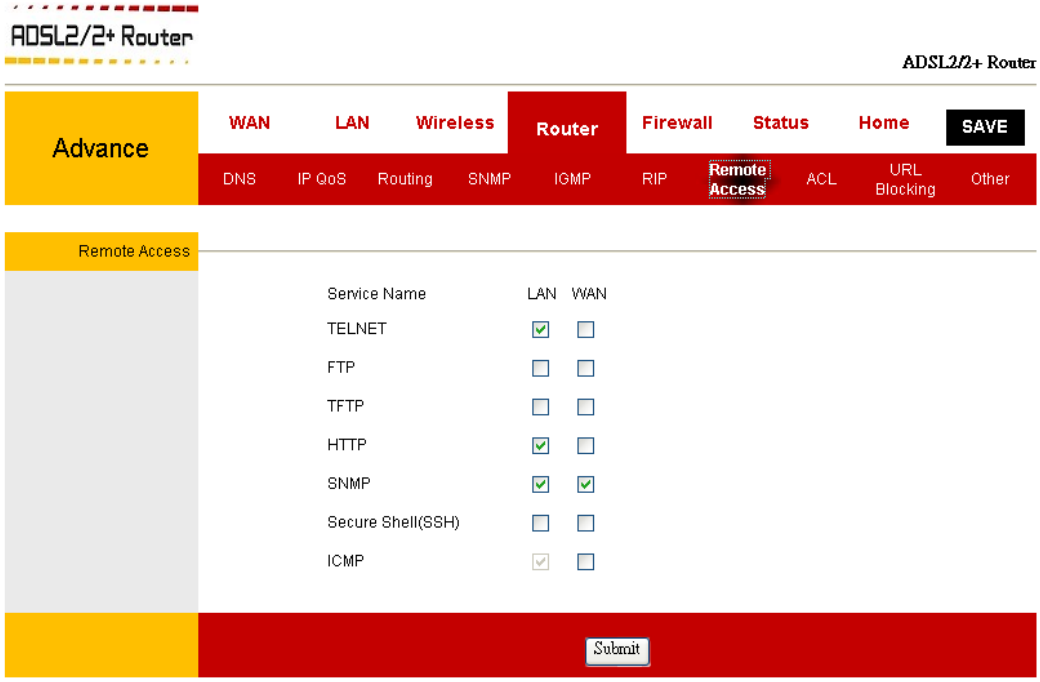
- **Interface:** Name of the interface on which you want to enable RIP.
- **Add:** Click **Add** to complete the setting. The new RIP entry will display in the table.

4.4.4.7 Advance – Router – Remote Access

Remote Access allows you to open the access from the Internet (WAN) or LAN to the following management ports of this 4 Ports 11g Wireless ADSL2/2+ Router:

- Telnet
- FTP
- TFTP
- HTTP
- SNMP
- Secure Shell (SSH)
- ICMP

Figure below illustrates the default **Remote Access** Control screen. The Remote Access is disabled by default, remote management from the WAN side IP addresses is denied, most services from the LAN side IP addresses are enabled.

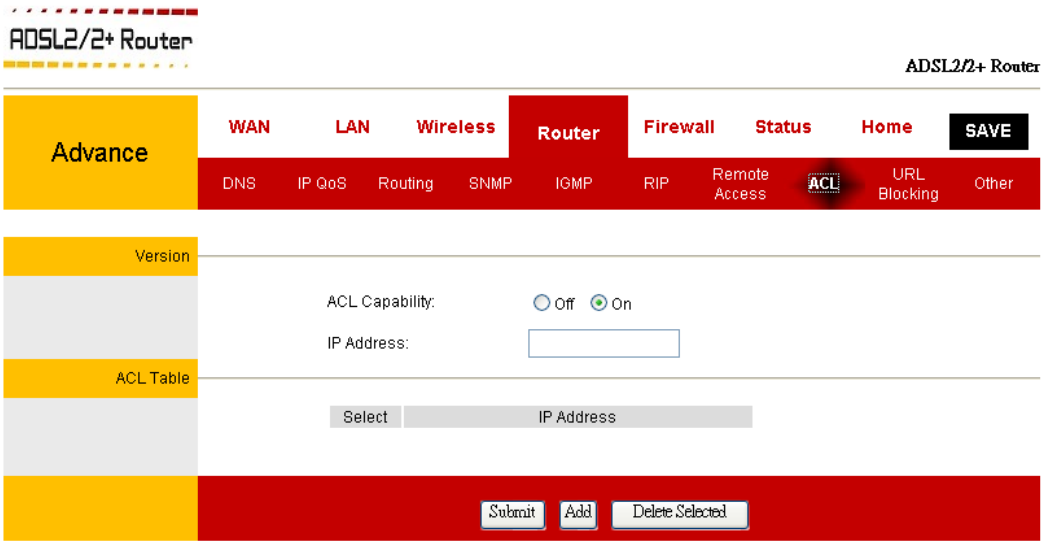


- **Submit:** Click **Submit** to complete the setting.

- To complete and save the setting, click **SAVE** after clicking the **Submit** button.

4.4.4.8 Advance – Router – ACL

The **ACL** (Access Control List) page enables you to specify which LAN/WAN IP addresses are allowed access to this 4 Ports 11g Wireless ADSL2/2+ Router configuration services specified.

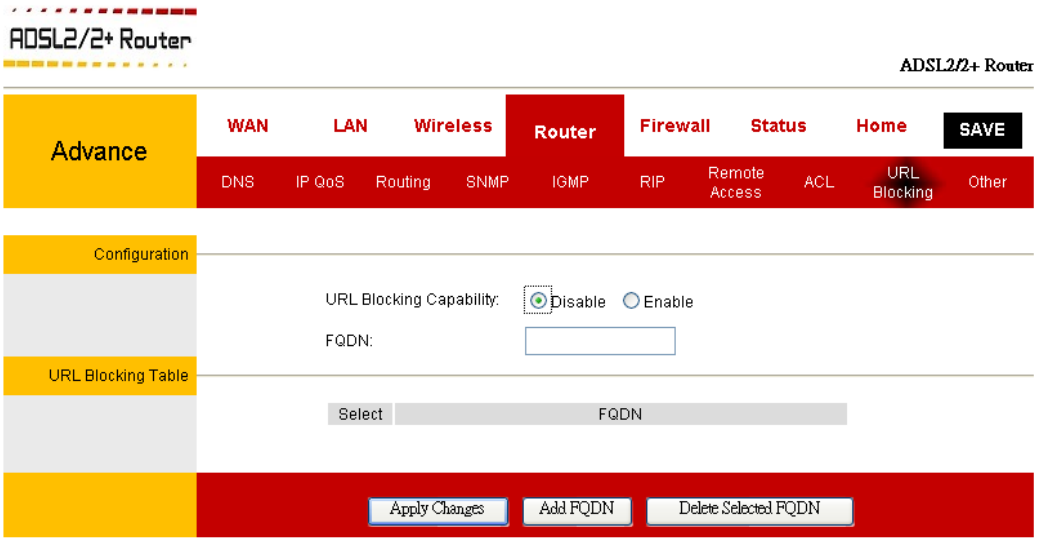


- **ACL Capability:** Check to turn ON or OFF the ACL capability.
- **IP Address:** Add new IP Access to the list.
- **Submit:** Click **Submit** to complete the setting.
- **Add:** Click **Add** and add in new ACL list.
- **Delete Selected:** Delete the selected ACL List from the table.
- To complete and save the setting, click **SAVE** after clicking the **Submit** button.

4.4.4.9 Advance – Router – URL Blocking

A URL is a web address that is normally typed into a web browser. For instance www.yahoo.com, www.msn.com are all URLs. URL Blocking allows you to block URLs based upon keywords that you enter into a box. Blocking URLs prevents people on your network from accessing these websites. These keywords may be full URL's or they may just be words.

FQDN (Fully Qualified Domain Name) means the complete domain name for a specific computer (host) on the Internet. It provides enough information so that it can be converted into a physical IP address. The FQDN consists of host name and domain name. For example, **www.google.com** is the FQDN on the Web for the publisher of this database. The **WWW** is the host. On the Web, there are millions of hosts named WWW in order to maintain uniformity. **GOOGLE.COM** is the domain name, with **.COM** being the top level domain (TLD) name.

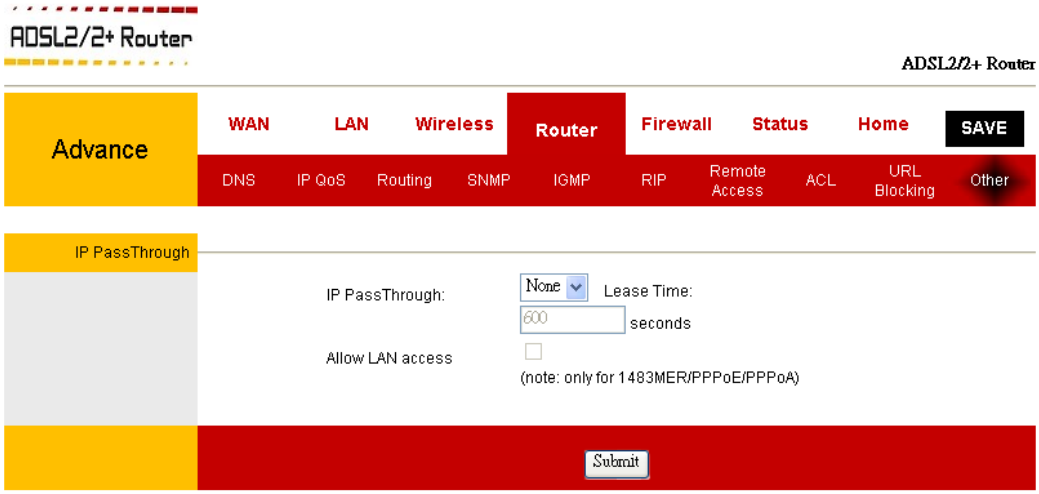


- **URL Blocking Capability:** Check to turn ON or OFF the URL Blocking capability.
- **FQDN:** The complete domain name for a specific computer (host) on the Internet.
- **Apply Changes:** Click **Apply Changes** to confirm your setting.
- **Add FQDN:** Click **Add FQDN** and add in new list.
- **Delete Selected FQDN:** Delete the selected FQDN List from the table.
- To complete and save the setting, click **SAVE** after clicking the **Submit** button.

4.4.4.10 Advance – Router – Other

IP Pass Through: Although the Router mode is capable of terminating the PPP in the modem and hence does not require PPPoE client software on the host PC, there are some disadvantages to Router mode when only single-user support is required. For instance, Router mode uses NAT which requires ALG support. **IP Pass Through** also terminates the PPP in the modem and does not require a PPPoE client on the PC. However, **IP Pass Through** does not use NAT and is not limited by ALGs. **IP Pass Through** will work with Ethernet interface to the PC.

When **IP Pass Through** is enabled, only one PC is able to access the Internet, and the DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only the PC with the WAN IP address can access the Internet.



- **IP Pass Through:** Select the WAN connection profile from the drop down manual on which the rule will take effect.
- **Lease time:** The Lease time is the amount of time a network user will be allowed to connect with DHCP server.
- **Allow LAN access:** Click to enable **LAN Access**.
- **Submit:** Click **Submit** to complete the setting.
- To complete and save the setting, click **SAVE** after clicking the **Submit** button.

4.4.5 Advanced – Firewall

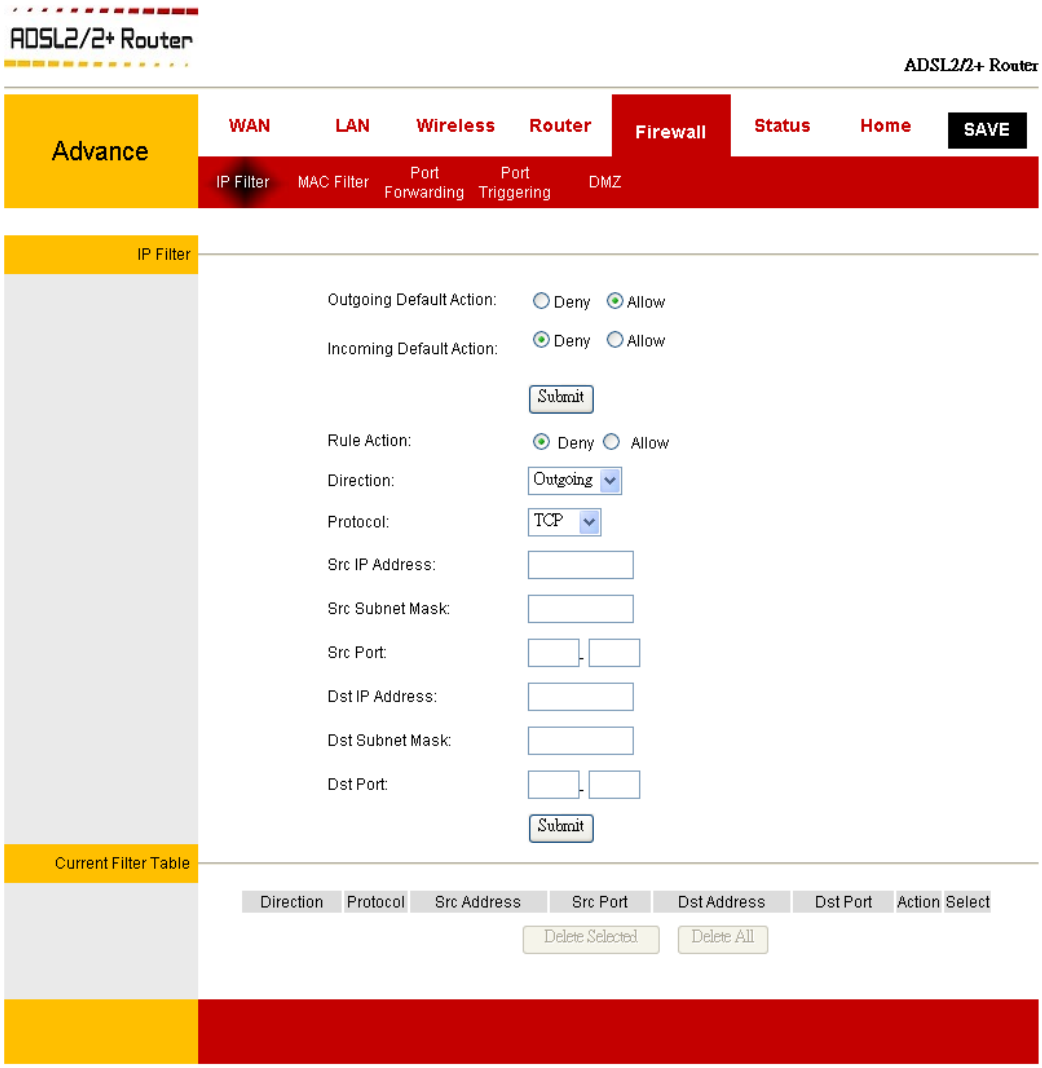
A **Firewall** is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

4.4.5.1 Advanced – Firewall – IP Filter

The **IP Filter** feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN. You can create **IP Filter** rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN.

When you define an **IP Filter** rule and enable the feature, you instruct the 4 Ports 11g Wireless ADSL2/2+ Router to examine data packets to determine whether they meet criteria set forth in the rule. The criteria can include the network or internet protocol the packet carries, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data. If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

Click the **Advance – Firewall** tab, and then click **IP Filter** in the task bar, the following window will pop-up.



■ IP Filter:

- ☑ **Outgoing Default Action:** Click **Allow** or **Deny** the outgoing action.
- ☑ **Incoming Default Action:** Click **Allow** or **Deny** the incoming action.
- ☑ **Rule Action:** Specifies what the rule will do to a packet when the packet matches the rule criteria. The action can be **Allow** (forward to destination) or **Deny** (discard the packet).
- ☑ **Direction:** Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface. Incoming refers to packets coming in to the LAN on the interface, and Outgoing refers to packets going out from the LAN. You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.
- ☑ **Protocol:** IP protocol criteria that must be met for rule to be invoked. You can specify that packets must contain the selected protocol, that they must not contain the specified protocol, or that the rule can be invoked regardless of the protocol. TCP, UDP, and ICMP are common IP protocols.
- ☑ **Src IP Address:** IP address criteria for the source computer(s) from which the packet originates.
- ☑ **Src Subnet Mask:** The Subnet Mask of the source IP on your LAN side.
- ☑ **Src Port:** Port number (Start Port and End Port) criteria for the source computer(s). Port numbers identify the type of traffic that the computer or server can handle and are specified by the Internet Assigned Numbers Authority (IANA). These fields will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol.
- ☑ **Dst IP Address:** IP address rule criteria for the destination computer(s) (i.e., the IP address of the computer to which the packet is being sent).
- ☑ **Dst Subnet Mask:** The destination computer(s) subnet mask.
- ☑ **Dst Port:** Port number (Start Port and End Port) criteria for the destination computer(s). Port numbers identify the type of traffic that the computer or server can handle and are specified by the Internet Assigned Numbers Authority (IANA). These fields will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol.
- ☑ **Submit:** Click **Submit** to confirm your setting.

■ Current Filter Table:

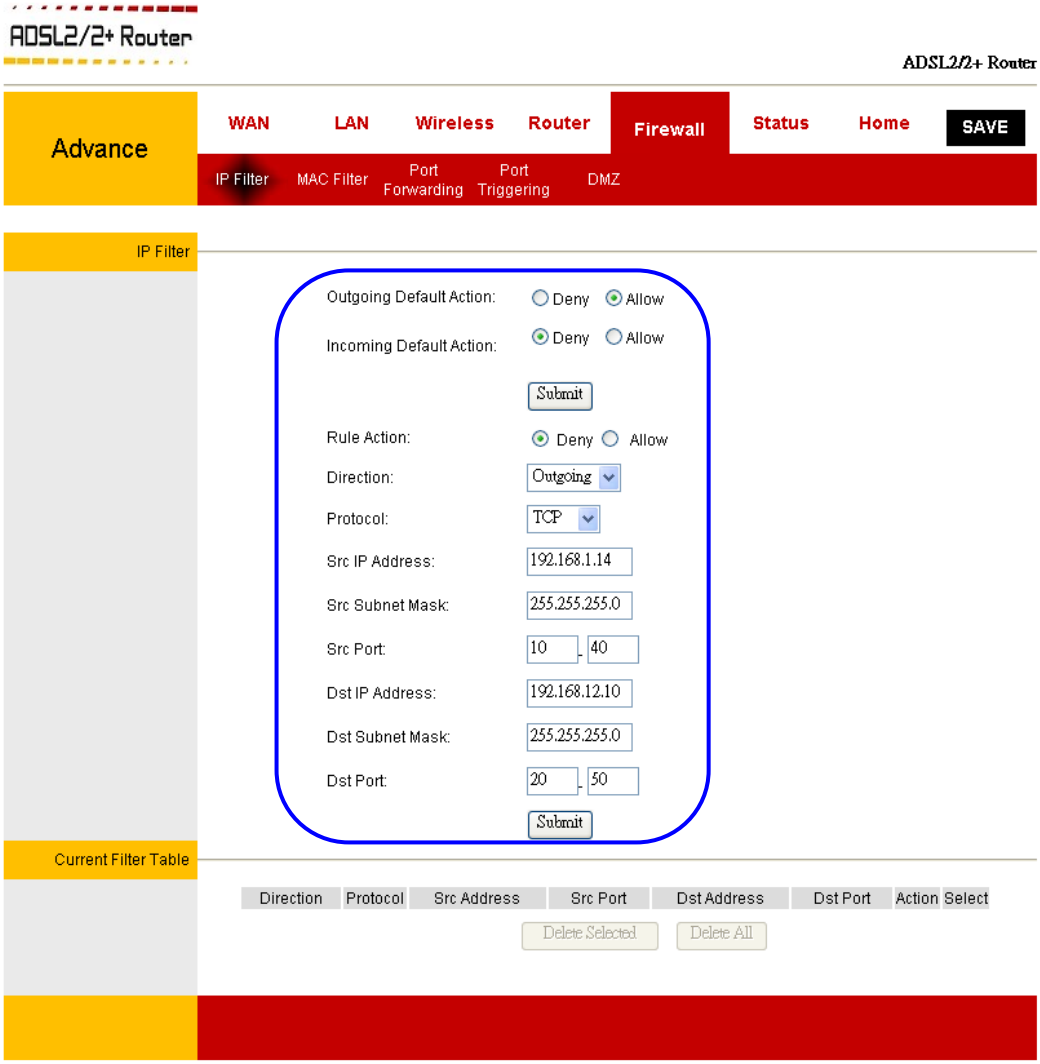
- ☑ IP Filter rules created.

4.4.5.1.1 Creating IP Filter Rules

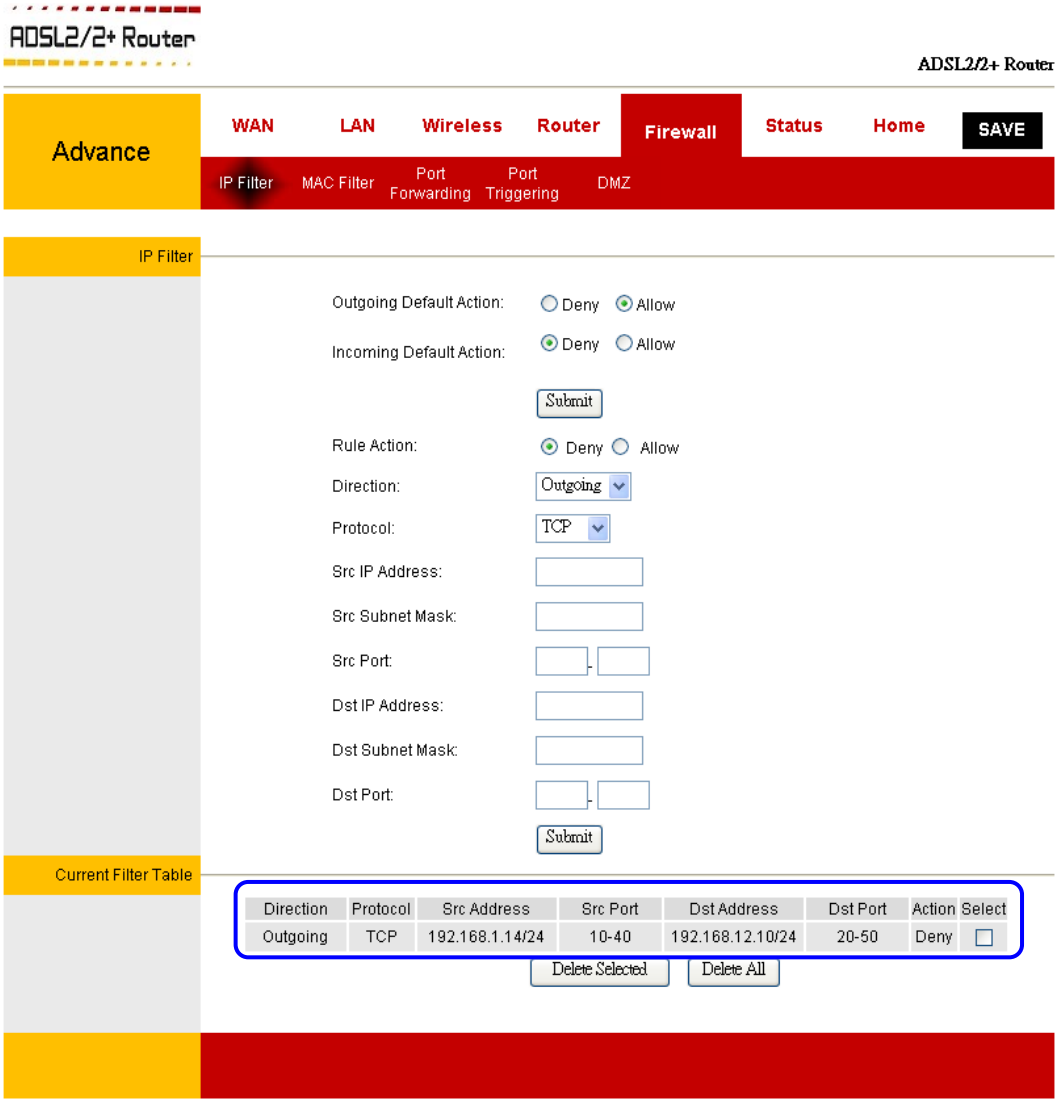
To create an IP filter rule, you set various criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule.

1. On the main **IP Filter** page, the following window screen will pop-up.

2. Enter or select data for each field that applies to your rule. Refer to previous section on the IP Filters Field Descriptions.



3. Click Submit after setup. The following screen display after Submit your rule.



4. You can **Delete Selected** or **Delete All** IP Filter Rules from the Current Filter Table. When you delete a session, the communication is discontinued.

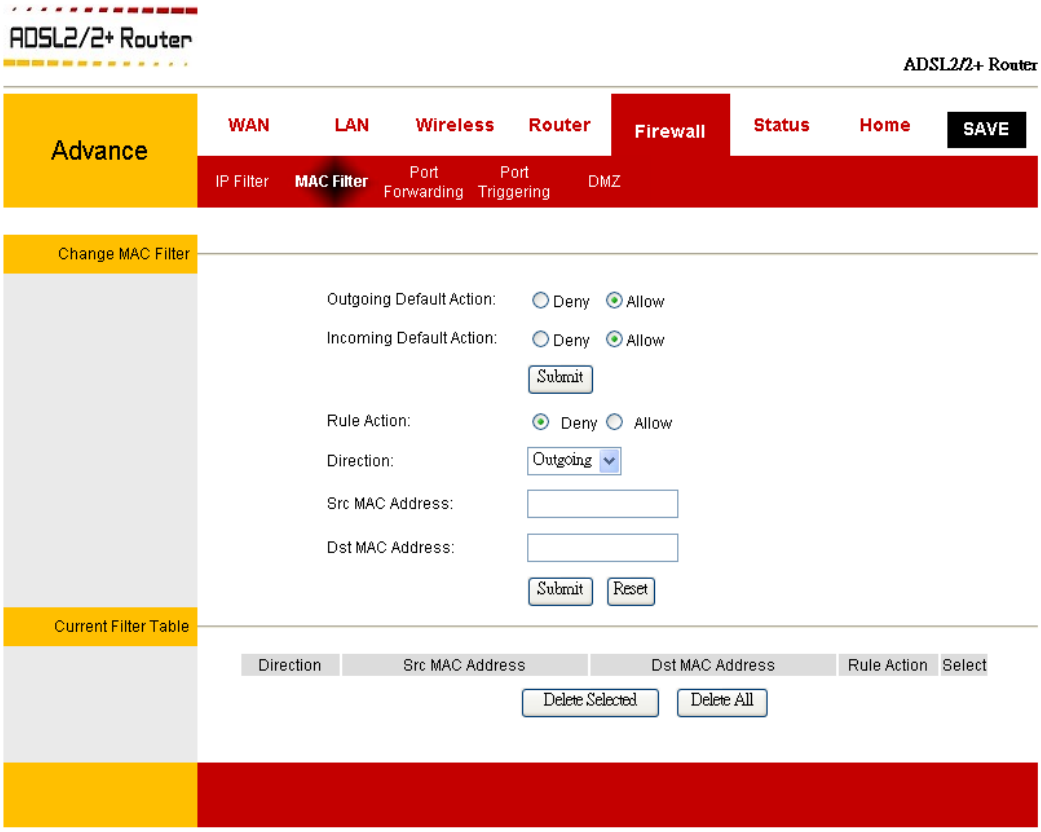
5. To make the change permanent, click on **SAVE** button.

4.4.5.2 Advanced – Firewall – MAC Filter

The **MAC Filtering** mechanism provides a way for you to define rules to allow or deny frames through the bridge based on source MAC address and destination MAC address.

When **MAC Filtering** is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed.

Note that the **MAC Filter** only examines frames from interfaces that are part of the bridge itself. Click on **Advanced – MAC Filter** tab, the following screen display. The **MAC Filter** page allows you to enable, add, edit, or delete the filter rules.



■ Change MAC Filter:

☑ **Outgoing Default Action:** Click **Allow** or **Deny** the outgoing action.

☑ **Incoming Default Action:** Click **Allow** or **Deny** the incoming action.

☑ **Rule Action:** Specifies what the rule will do to a packet when the packet matches the rule criteria. The action can be **Allow** (forward to destination) or **Deny** (discard the packet).

- ☑ **Direction:** Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface. Incoming refers to packets coming in to the LAN on the interface, and Outgoing refers to packets going out from the LAN. You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.

- ☑ **Src MAC Address:** The source MAC address. It must be in a xxxxxxxxxxxx format, with 000000000000 as “don't care”.

- ☑ **Dst MAC Address:** The destination MAC address.

- ☑ **Submit:** Click **Submit** button to add the rule to the list of rules.

- ☑ **Reset:** Click **Reset** to ignore all the changes.

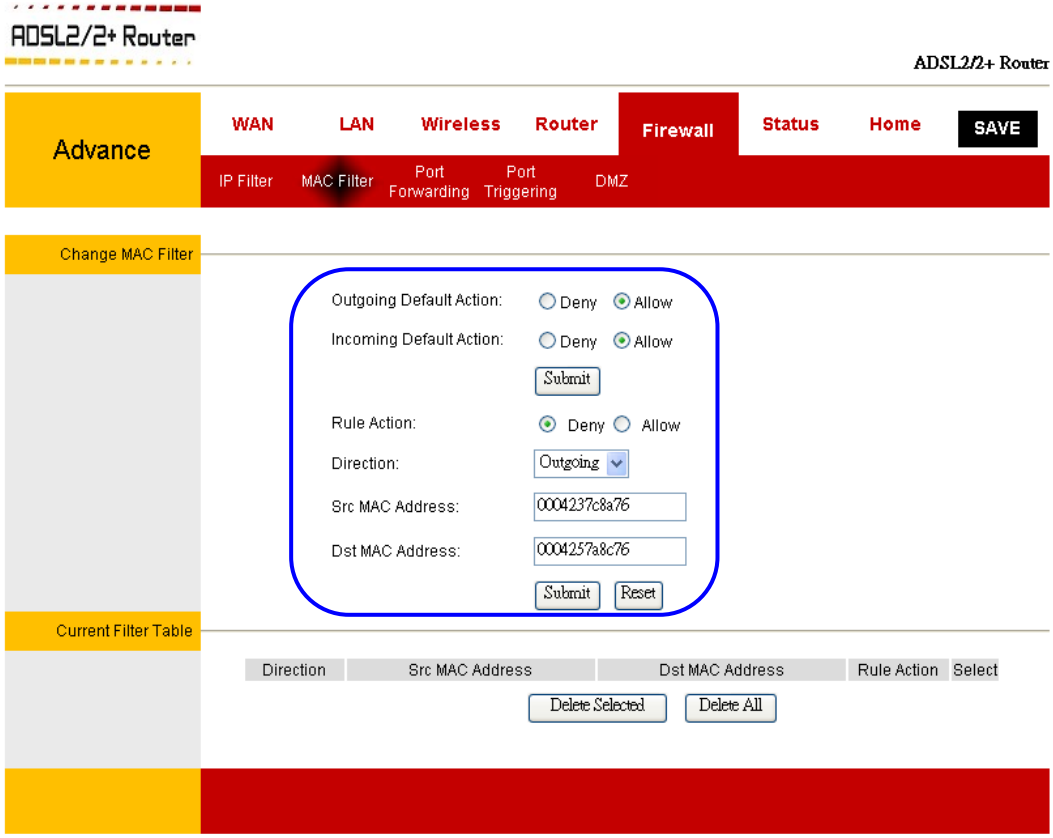
- ☑ To complete and save the setting, click **SAVE** button.

4.4.5.2.1 MAC Filters Configuration Procedure

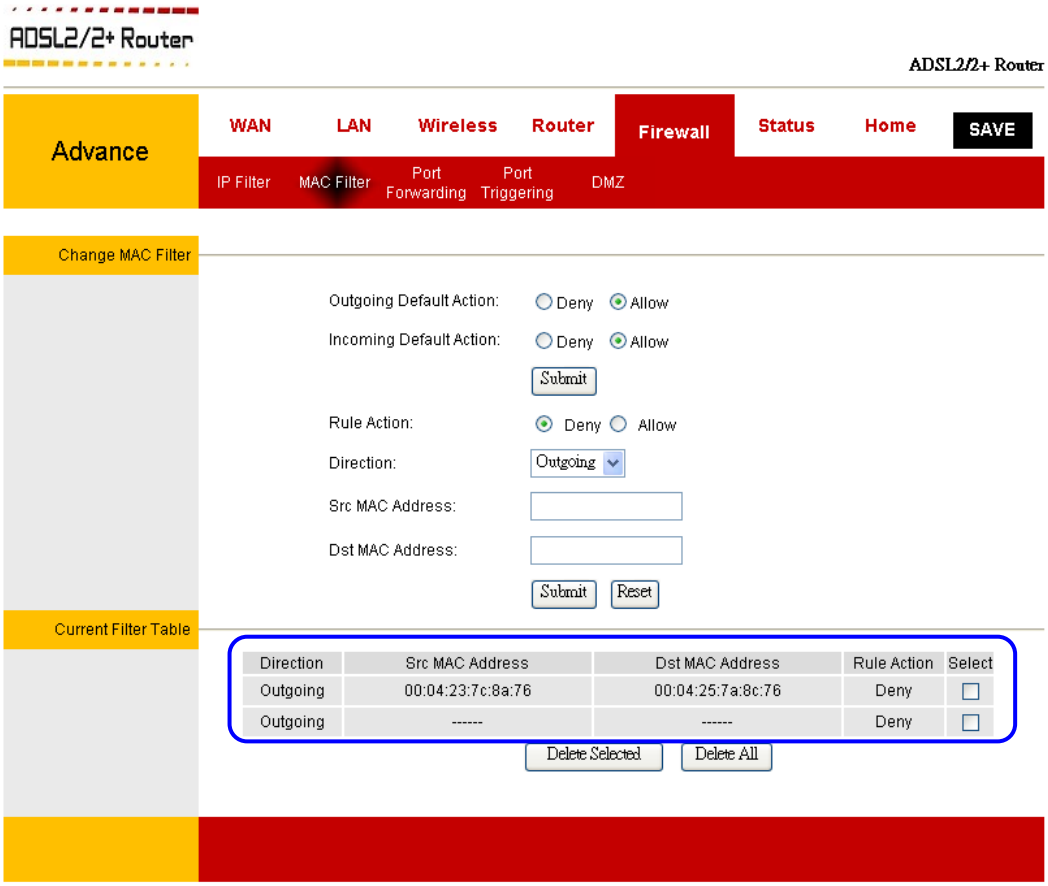
Use the following procedures to enable and configure MAC Filter.

1. Click the **Advance – Firewall – MAC Filter** tab to display the configuration homepage.

2. Enter or select data for each field that applies to your rule. Refer to previous section on the MAC Filter Field Descriptions.



3. Click **Submit** after setup. The following screen display after Submit your rule.



4. You can **Delete Selected** or **Delete All** IP Filter Rules from the Current Filter Table. When you delete a session, the communication is discontinued.

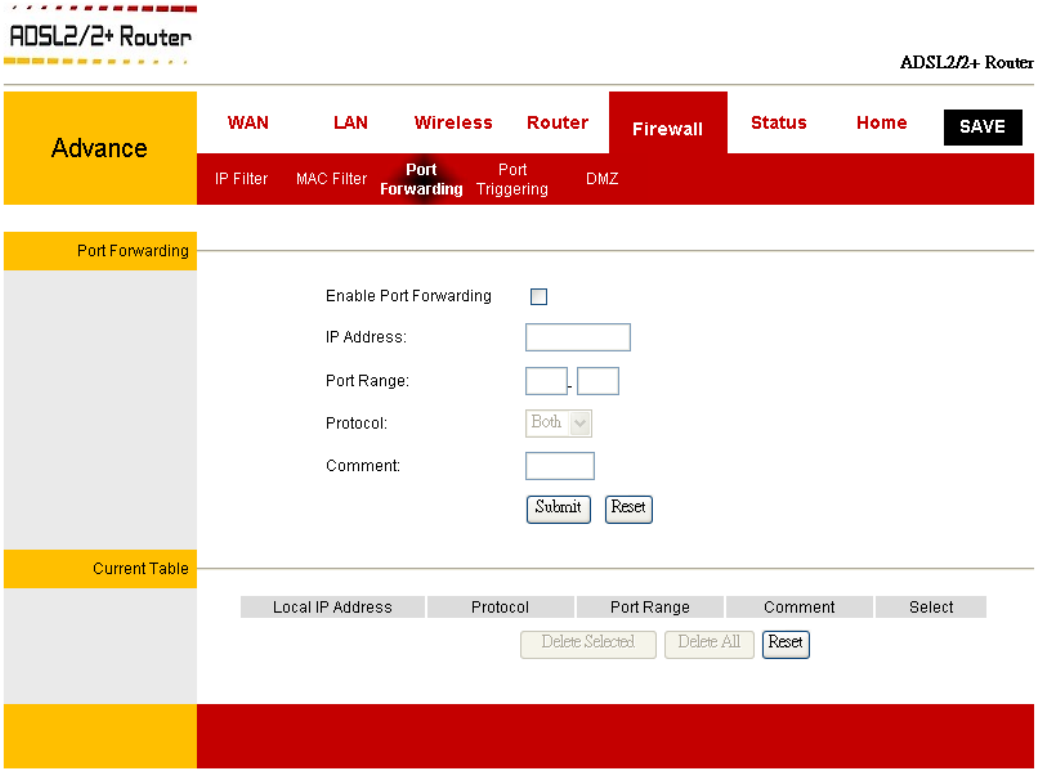
5. To make the change permanent, click on **SAVE** button.

4.4.5.3 Advanced – Firewall – Port Forwarding

Port Forwarding (or Virtual Server) allows you to direct incoming traffic to specific PCs based on a service port number and protocol. Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games.

A database of predefined Port Forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category, and add the available rules for a given category. You can also create/delete your own Port Forwarding rules.

Click on Advance – Firewall – Port Forwarding tab, the following configuration page display.



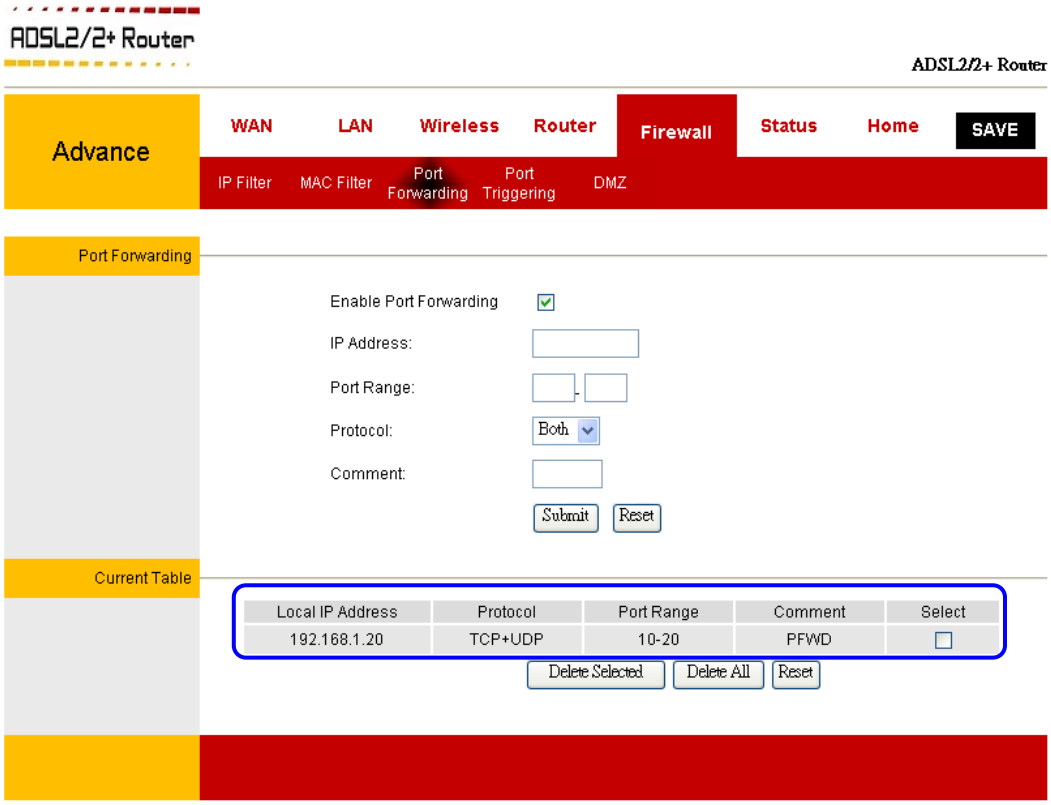
- **IP Address:** The IP address from which the incoming traffic is allowed.
- **Port Range:** The starting port and ending port number that will be blocked for this application.
- **Protocol:** There are 3 options available: TCP, UDP and Both.
- **Comment:** The Port Forwarding name.
- **Submit:** Click Submit to confirm your setting.
- **Reset:** Click Reset to give up any changes.

4.4.5.3.1 Port Forwarding Configuration Procedure

1. From the **Port Forwarding** configuration screen, check to enable Port Forwarding feature.

2. Manually enter or select the **IP Address**, **Port Range**, **Protocol** and **Comment**. Click Submit after setup. The following screen display.

   Note: The IP Address should be set within the current subnet. The **Delete Selected**, **Delete All**, and **Reset** buttons become available only when the **Port Forwarding** category is created.

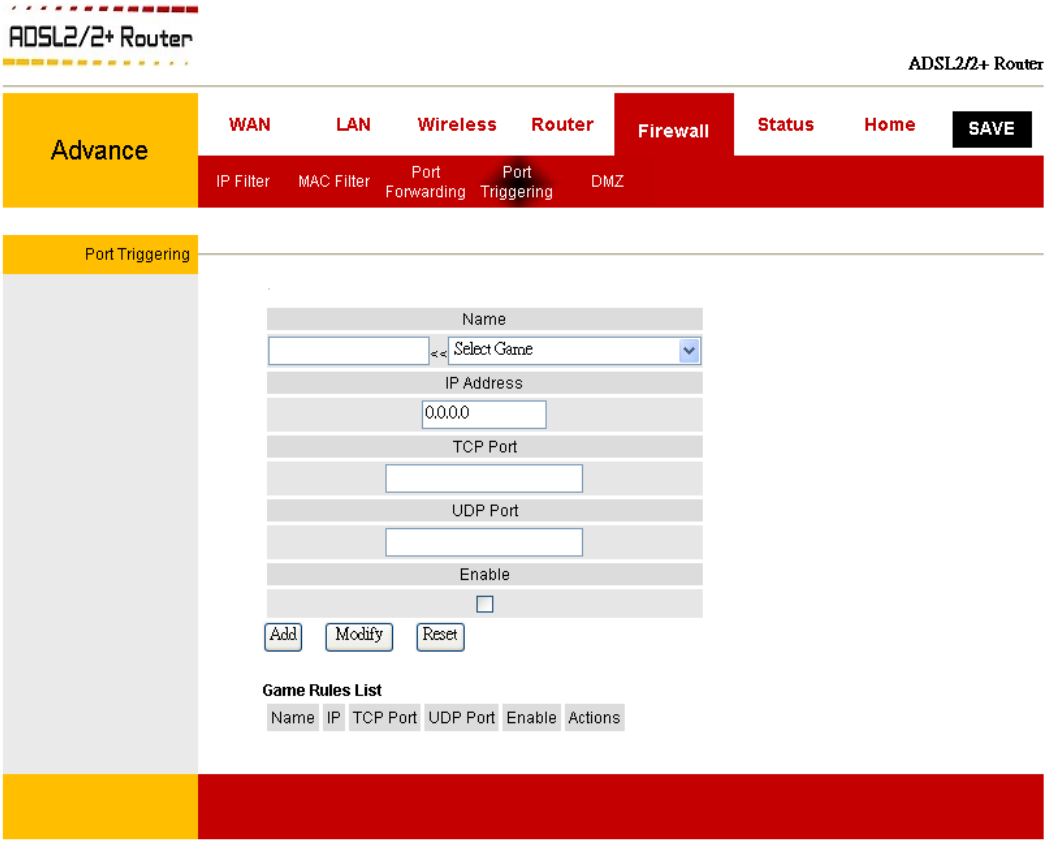


3. To make the change permanent, click **SAVE**.

4.4.5.4 Advanced – Firewall – Port Triggering

Port triggering is a specialized form of **Port Forwarding** which allows computers behind a NAT-enabled router dynamic hosts on a local network to provide services which would normally require a static host (a host with an unchanging network address). **Port Triggering** triggers an open incoming port when a client on the local network makes an outgoing connection to a predetermined port on a server.

Similar to standard **Port Forwarding**, it allows a client to connect to a host behind a NAT router. The disadvantage of **Port Forwarding** is that it only allows one client on the network to use a particular service that occupies a particular port. **Port Triggering** is unsuitable for having servers behind a NAT router (you want standard port forwarding) because it relies on the computer to make an outgoing connection before it can receive incoming ones. Click on **Advance – Firewall – Port Triggering** tab, the following screen display:



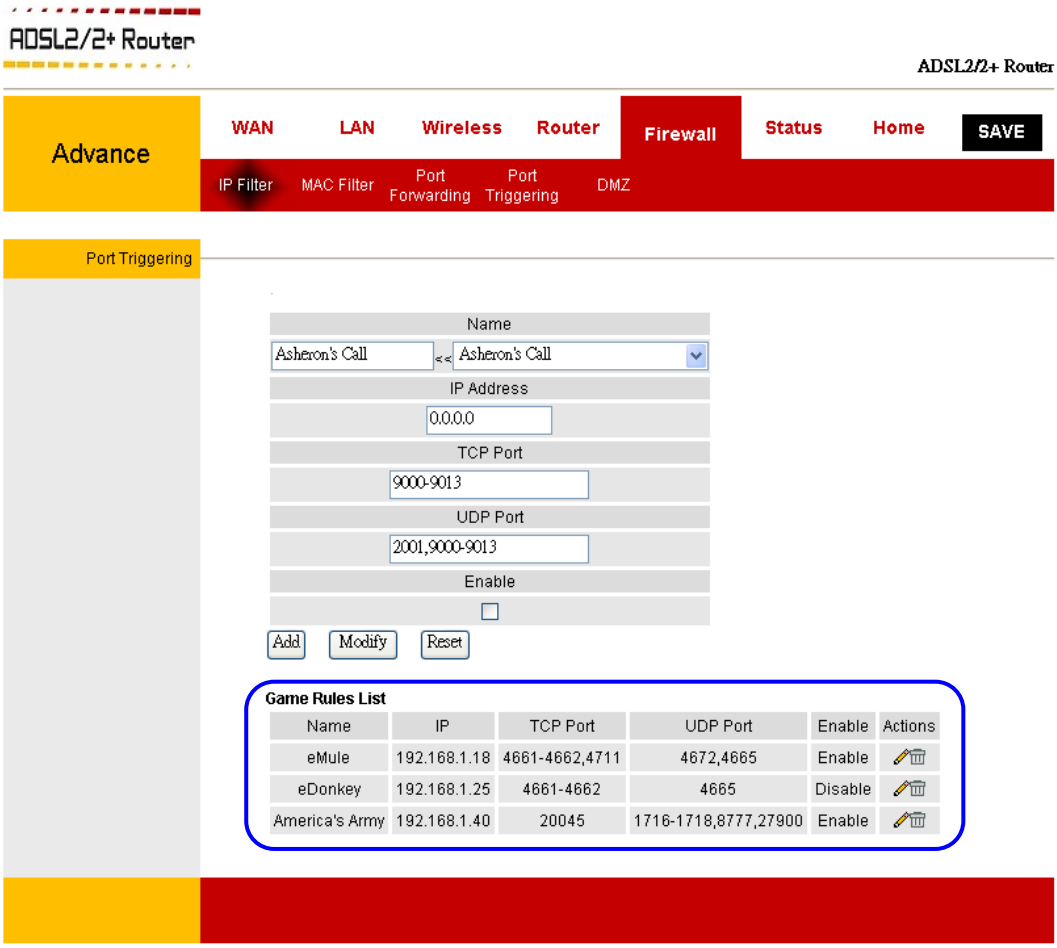
- **Name:** Select the predefined rules from the drop down manual.
- **IP Address:** The IP Address which should be set within the current subnet.
- **TCP Port:** The preset TCP Port of the selected rules.
- **UDP Port:** The preset UDP Port of the selected rules.
- **Enable:** Place a check (Enable) or uncheck (Disable) the Port Triggering Rule.
- **Add:** Click Add button to add the Port Triggering rule to the Game Rule Table.
- **Modify:** Modify the Port Triggering Rule.
- **Reset:** Give up your changes.

4.4.5.4.1 Port Triggering Configuration Procedure

6. From the **Port Triggering** configuration screen, select the triggering Name from the predefine drop down manual.

7. Enter the current subnet **IP Address**. The IP Address should be set within the current subnet.

8. Place a check (Enable) or uncheck (Disable) the Port Triggering Rule. Click Add after setup. The following screen display.

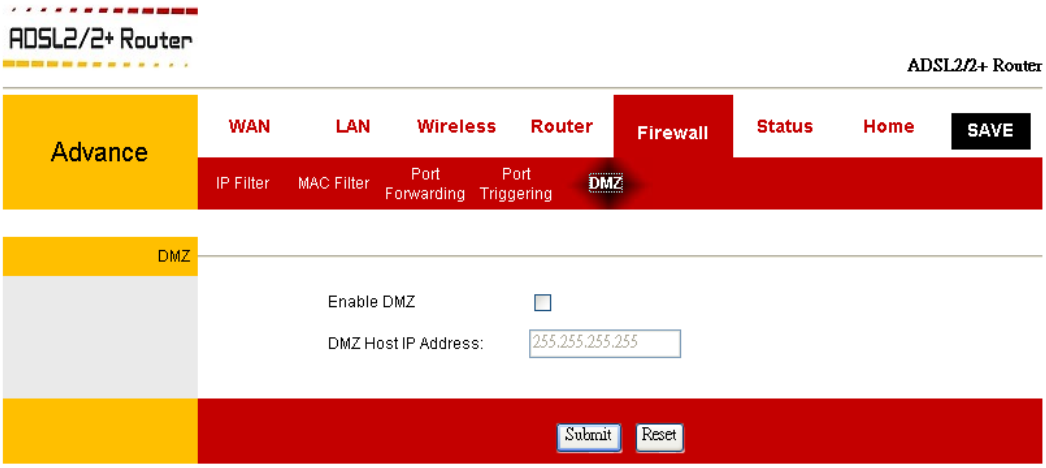


9. The Action column provides icons you can click on to modify ( ) or delete ( ) the Port Triggering Rules.

4.4.5.5 Advanced – Firewall – DMZ

Setting a host on your local network as demilitarized zone (**DMZ**) forwards any network traffic that is not redirected to another host via the port forwarding feature to the IP address of the host. This opens the access to the DMZ host from the Internet. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall.

Click on the Advance – Firewall – DMZ tab, the following DMZ configuration page display:



- **Enable DMZ:** Place a check to enable the DMZ functionality.

- **DMZ Host IP Address:** Select the LAN IP address you are going to use as the DMZ host. This host is exposed to the Internet. Be aware that this feature may expose your local network to security risks.

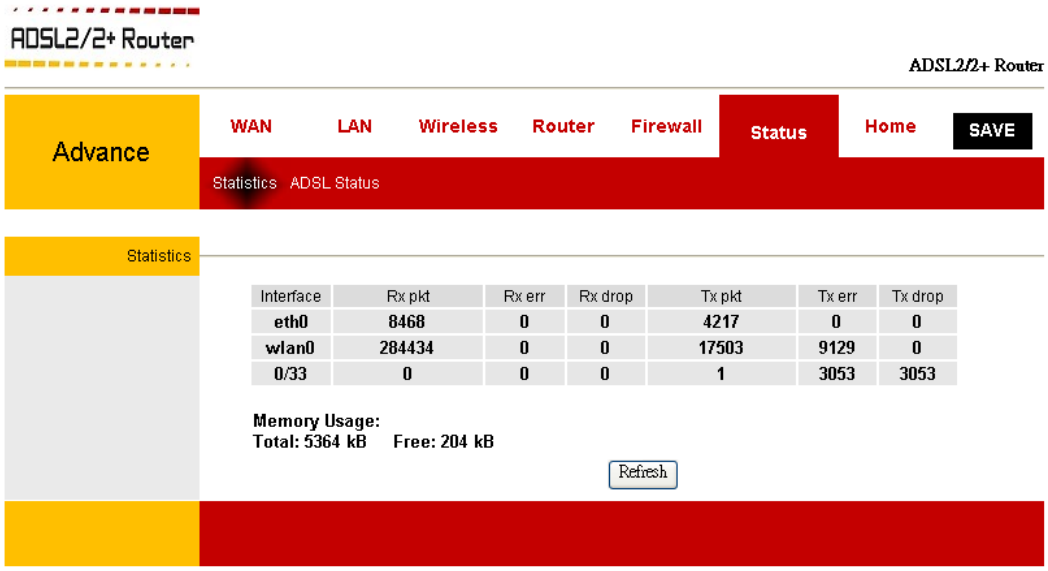
- **Submit:** Click Submit button to confirm your setting.

- **Reset:** Give up your changes.

4.5 Advance – Status

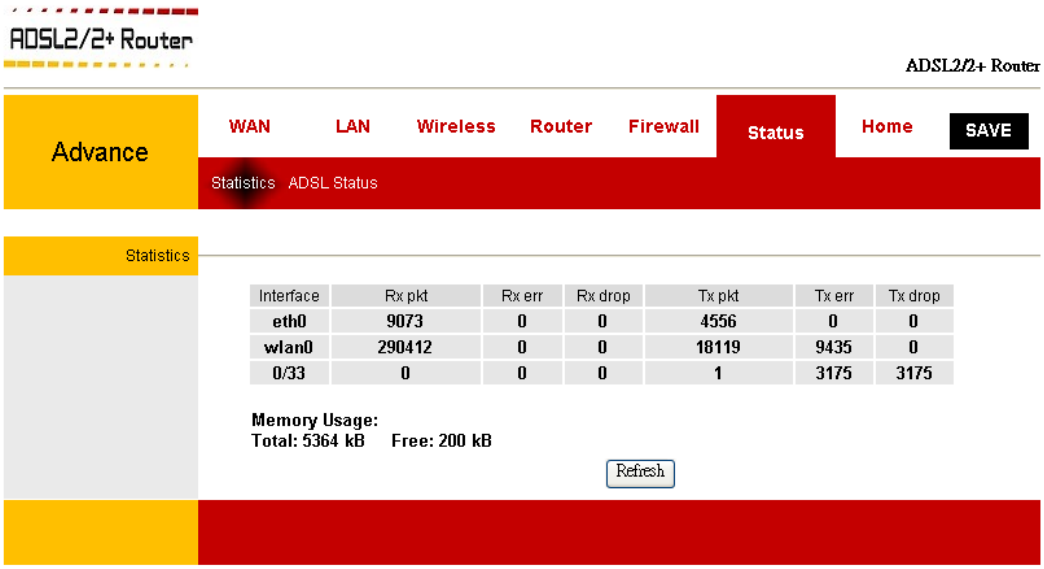
Figure below shows the **Status** main screen, which can be accessed by clicking on the **Advance – Status** tab from the top of the screen. This screen provides access to the following status screens:

- Network Statistics
- ADSL Status



4.5.1 Advance – Status – Statistic

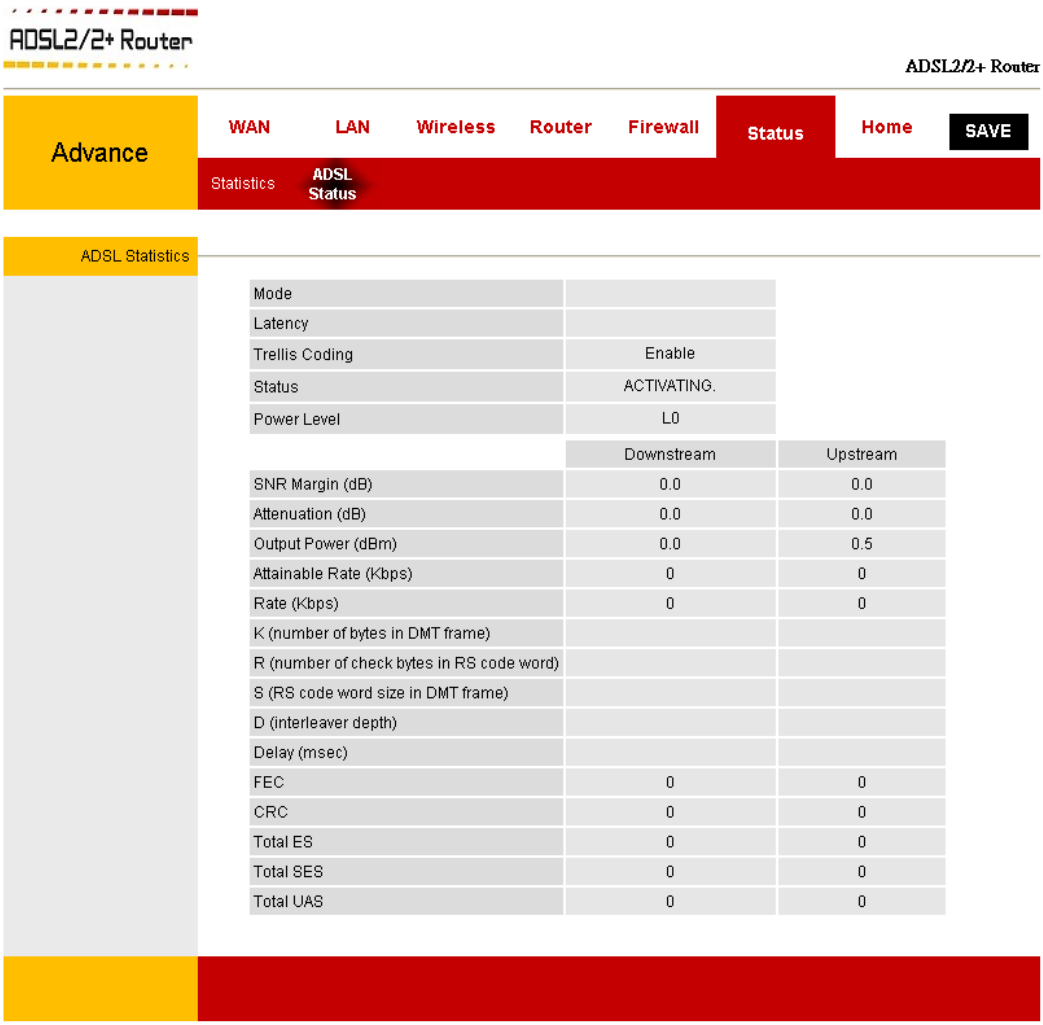
The **Status – Statistic** page shows the status of each PPP session for each PPP interface. This page contains information that is dynamic and will refresh every 10 seconds.



- **Interface:** States the interface that is being used (Ethernet, Wireless LAN, ADSL WAN connection profile).
- **Rx pkt:** Number of packets received by a particular PPP connection.
- **Rx err:** Number of Error packets received by a particular PPP connection.
- **Rx Drop:** Number of packets drop by a particular PPP connection.
- **Tx pkt:** Number of packets sent by a particular PPP connection.
- **Tx pkt:** Number of packets sent by a particular PPP connection.
- **Tx err:** Number of Error packets sent by a particular PPP connection.
- **Memory Usage:** The 4 Ports 11g Wireless ADSL2/2+ Router's system memory.
- **Refresh:** Click **Refresh** button to reload Web browser.

4.5.1 Advance – Status – ADSL Status

The **ADSL Status** page shows the 4 Ports 11g Wireless ADSL2/2+ physical layer or link status. The information displayed on this page is either inherent to the 4 Ports 11g Wireless ADSL2/2+ Router or set by the ADSL Central Office (CO) DSLAM, neither of which cannot be changed by the user.



Appendix A: Router Terms

What is a firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

What is NAT?

NAT stands for Network Address Translation. Another name for it is Connection Sharing. What does this mean? Your ISP provides you with a single network address for you to access the Internet through. However, you may have several machines on your local network that want to access the Internet at the same time. The router provides NAT functionality that converts your local network addresses to the single network address provided by your ISP. It keeps track of all these connections and makes sure that the correct information gets to the correct local machine.

Occasionally, there are certain programs that don't work well through NAT. Some games, and some specialty applications have a bit of trouble. The router contains special functionality to handle the vast majority of these troublesome programs and games. NAT does cause problems when you want to run a SERVER though. When running a server, please see the DMZ section below.

What is a DMZ?

DMZ really stands for Demilitarized Zone. It is a way of separating out part of your local network so that is more open to the Internet. Suppose that you want to run a web-server, or a game server. Normal servers like these are blocked from working by the NAT functionality. The solution is to "isolate" the single local computer into a DMZ. This makes the single computer look like it is directly on the Internet, and others can access this machine.

Your machine isn't really directly connected to the Internet, and it really has an internal local network address. When you provide the servers network address to others, you must provide the address of the router. The router "fakes" the connection to your machine.

You should use the DMZ when you want to run a server that others will access from the Internet. Internal programs and servers (like print servers, etc) should NOT be connected to the DMZ

What is a Gateway?

The Internet is so large that a single network cannot handle all of the traffic and still deliver a reasonable level of service. To overcome this limitation, the network is broken down into smaller segments or subnets that can deliver good performance for the stations attached to that segment. This segmentation solves the problem of supporting a large number of stations, but introduces the problem of getting traffic from one subnet to another.

To accomplish this, devices called routers or gateways are placed between segments. If a machine wishes to contact another device on the same segment, it transmits to that station directly using a simple discovery technique. If the target station does not exist on the same segment as the source station, then the source actually has no idea how to get to the target.

One of the configuration parameters transmitted to each network device is its default gateway. This address is configured by the network administrators and it informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside of this area, it is usually because of an incorrectly configured default gateway.

Appendix B: Frequently Asked Questions

The Frequently Asked Questions addresses common questions regarding 4 Ports 11g Wireless ADSL2/2+ Router settings.

Some of these questions are also found throughout the guide, in the sections to which they reference.

1. **How do I determine if a link between the Ethernet card (NIC) and the 4 Ports 11g Wireless ADSL2/2+ Router has been established?**

Ans. A ping test would determine if a connection is established between your 4 Ports 11g Wireless ADSL2/2+ Router and computer. Using, the ping command, ping the IP address of the 4 Ports 11g Wireless ADSL2/2+ Router, in this case, 192.168.1.1 (default). For more information on Ping Testing, refer to Appendix C: Troubleshooting Guide. Alternatively, if the Ethernet LINK LED is solidly on, then the Ethernet link is established.

2. **How do I determine if a link between the 4 Ports 11g Wireless ADSL2/2+ Router and the Internet has been established?**

Ans. Similar to the previous question, a ping test would determine whether or not a connection is established. However, this time use a URL instead of and IP Address, such as www.google.com. Alternatively, if the ADSL LED is solidly on, then the ADSL link is established.

3. **How can I find/verify my 4 Ports 11g Wireless ADSL2/2+ Router and/or computer Ethernet MAC Address?**

Ans. Refer to **Status – Info** section for details.

4. **I can't get the Internet game, server, or application to work properly.**

Ans. If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one computer to the Internet using DeMilitarized Zone (DMZ) setting. Refer to **Advanced – Port Forwarding** section for the setting detail.

5. **I need to upgrade the firmware.**

Ans. In order to upgrade the firmware with the latest features, check with your local dealer or ISP for technical support.

6. I forgot my password.

Ans. Reset the 4 Ports 11g Wireless ADSL2/2+ Router to factory default by pressing the Reset button for 10~15 seconds and then releasing it.

If you are still getting prompted for a password when saving settings, then perform the following steps:

1. Access the 4 Ports 11g Wireless ADSL2/2+ Router's web-based utility by going to http://192.168.1.1 or the IP address of the 4 Ports 11g Wireless ADSL2/2+ Router. Enter the default username and password **Admin**, and click the **Tools – User Management** tab.
2. Enter a different password in the 4 Ports 11g Wireless ADSL2/2+ Router Password field, and enter the same password in the second field to confirm the password.
3. Click the **Apply** button then click **Save All** to activate your setting.

7. What is ad-hoc mode?

Ans. When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured To communicate directly with each other, peer-to-peer without the use of an access point.

8. What is infrastructure mode?

Ans. When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a network through a wireless access point.

9. What is roaming?

Ans. Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the computer must make sure that it is the same channel number with the access point of dedicated coverage area.

10. What is ISM band?

Ans. The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

11. What is MAC Address?

Ans. Short for **Me**dia **A**ccess **C**ontrol Address. It is a hardware address that uniquely identifies each node of a Ethernet networking device. This address is usually permanent.

12. What is IEEE 802.11b standard?

Ans. IEEE 802.11b is an extension standards to 802.11 that applies to Wireless LAN and provides 11Mbps transmission speed in the 2.4 GHz band.

13. What is IEEE 802.11g standard?

Ans. IEEE 802.11g is an extension standards to 802.11 that applies to Wireless LAN and provides 54Mbps transmission speed in the 2.4 GHz band.

14. What is NAT (Network Address Translation) and what is it used for?

Ans. NAT translates multiple IP Address on the private LAN to one public IP Address (in WAN) that is sent out to the Internet. NAT adds a level security since the IP address of a PC connected to the private LAN is never transmitted on the Internet.

15. What can I do when I am not able to get the web configuration screen for this 4 Ports 11g Wireless ADSL2/2+ Router?

Ans. Remove the proxy settings on your Internet Browsers or remove the dial-up settings on your browser.

16. What is DMZ (DeMilitarized zone)?

Ans. DMZ allows one IP Address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ features.

17. What is BSS ID?

Ans. A specific Ad-Hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

18. What is SSID?

Ans. Short for Service Set Identifier. SSID is a 32 character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all Access Point and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID.

19. What is WEP?

Ans. Short for **W**ired **E**quivalent **P**rivacy. WEP is a security protocol for wireless local area networks defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

17. **What is WPA?**

Ans. Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

18. What is the maximum IP addresses supported by this 4 Ports 11g Wireless ADSL2/2+ Router?

Ans. The 4 Ports 11g Wireless ADSL2/2+ Router can support up to 253 IP addresses.

Appendix C: Troubleshooting Guide

The Troubleshooting Guide provides answers to common problems regarding the 4 Ports 11g Wireless ADSL2/2+ Router settings, connections, and computer settings.

1. The 4 Ports 11g Wireless ADSL2/2+ Router does not work (None of the LEDs light up)

Ans. Check the following:

1. Make sure that the 4 Ports 11g Wireless ADSL2/2+ Router is plugged into a power socket.
2. Make sure that you are using the correct power supply for your 4 Ports 11g Wireless ADSL2/2+ Router device.
3. Make sure the power switch on the 4 Ports 11g Wireless ADSL2/2+ Router is turned on.

2. I changed the LAN IP Address in the LAN configuration page and my PC is no longer able to detect the 4 Ports 11g Wireless ADSL2/2+ Router.

Ans. After changing the LAN IP Address of the 4 Ports 11g Wireless ADSL2/2+ Router, proceed to the following step before a PC is able to recognize the 4 Ports 11g Wireless ADSL2/2+ Router:

1. Click **"Start"** → **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.
3. In the command prompt, type **"ipconfig/release"** then press **"Enter"** (For Windows 2000/XP Operating System).
4. Type **"ipconfig/renew"** then press **"Enter"**.

3. No wireless connectivity.

Ans. Check the following:

1. Make sure both wireless client adapter and the 4 Ports 11g Wireless ADSL2/2+ Router is allowed to connect through wireless channels as defined for local regulatory domain.
2. Make sure that the WLAN client is configured for the correct wireless settings (SSID, WEP).

4. Poor wireless connectivity or reach.

Ans. Check the following:

1. Choose automatic channel selection or be careful to select a DSSS channel that doesn't interfere with other radio channels.
2. Check the location of the 4 Ports 11g Wireless ADSL2/2+ Router in the building.
3. Make sure both WLAN client adapter and the 4 Ports 11g Wireless ADSL2/2+ Router is allowed to connect through wireless channels as defined for local regulatory domain.

5. LAN (Link/Act) LED does not light up.

Ans. Check the following:

1. Make sure that the LAN cables are securely connected to the 10/100Base-T port.
2. Make sure that you are using the correct cable type for your Ethernet equipment.
3. Make sure the computer's Ethernet port is configured for auto-negotiation.

6. Failed to configure the 4 Ports 11g Wireless ADSL2/2+ Router through web browser (By a client PC in LAN)

Ans. Check the following:

1. Check the hardware connection of the 4 Ports 11g Wireless ADSL2/2+ Router's LAN port. The LED will lit when a proper connection is made.
2. Check your Windows TCP/IP setting (Refer to Chapter 3 for setting details).
3. Open the Windows System Command Prompt:
   - For Windows 9x/ME: Manually enter **winipcfg**, then press **Enter**.
   - For Windows 2000/XP: Manually enter **ipconfig/all**, then press **Enter**.
4. You should have the following information listed on your Window System:
   - **IP Address: 192.168.1.x**
   - **Submask: 255.255.255.0**
   - **Default Gateway IP: 192.168.1.1**

7. I forgot or lost my Administrator Password.

Ans. Reset the 4 Ports 11g Wireless ADSL2/2+ Router to factory default by pressing the **"Reset"** button for 10~15 seconds.

If you are still getting prompted for a password when saving settings:

1. Access the Router's web interface by going to **http://192.1681.1.**
2. Enter the default **"username"** and **"password"** then click **"Enter"** to log in.
3. Click on **"Tools"** then click "**User Management"**.
4. Enter a new **"Password"** and new **"Username"** in the **"Username"** and "**Password"** field, and enter the same password in the second field to confirm the password.
5. Click **"Apply"** after setup then click **Save All** to activate your setting.

8. I need to upgrade the Firmware.

Ans. In order to upgrade the Firmware with the latest features, check your local dealer or ISP for technical support. Before proceed the upgrading process, check the following details:

1. Download the latest Firmware and save at your pointed location.
2. Read the firmware release note carefully before proceed the upgrading process.
3. Refer to **Tools - Update Gateway** section for the upgrading process.

9. Testing LAN path to your 4 Ports 11g Wireless ADSL2/2+ Router.

Ans. To verify whether the LAN path from your PC to your 4 Ports 11g Wireless ADSL2/2+ Router is properly connected, you can **"Ping"** the 4 Ports 11g Wireless ADSL2/2+ Router with the following procedures:

1. From the Windows toolbar, click **"Start"** and select **"Run".**
2. In the open field, type **"Ping 192.168.1.1"** and click **"OK"**
3. If the path is working, you should see the message in the following format:
   Reply from 192.168.1.1 bytes = 32 time < 10ms TTL = 60
4. If the path is not working, you should see the following message:
   Request timed out

If the path is not functioning correctly:

1. Make sure the LAN port LED indicator is on.
2. Check whether you are using the correct LAN cable.
3. Check your Ethernet Adaptor installation and configurations.
4. Verify that the IP address for your 4 Ports 11g Wireless ADSL2/2+ Router and your workstation are correct and that the addresses are on the same subnet.

10. Failed to connect with the 4 Ports 11g Wireless ADSL2/2+ Router via Wireless LAN card.

Ans. Ensure that the WL ACT LED indicator of the 4 Ports 11g Wireless ADSL2/2+ Router is correctly illuminated.

1. Check whether your Wireless LAN setting (e.g. SSID, Channel Number) is the same as your 4 Ports 11g Wireless ADSL2/2+ Router.
2. Check whether you'd used the same WEP Key Encryption for both your Wireless LAN and your 4 Ports 11g Wireless ADSL2/2+ Router.

Appendix D: Glossary

The Glossary provides an explanation of terms and acronyms discussed in this user guide.

10BASE-T: IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx: IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.11b: IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11g: IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11x: 802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys.

AP: Access Point: A station that transmits and receives data in a WLAN (Wireless Local Area Network). An access point acts as a bridge for wireless devices into a LAN.

ATM: Asynchronous Transfer Mode: A method of transfer in which data is organized into 53-byte cell units. ATM cells are processed asynchronously in relation to other cells.

BC: Broadcast: Communication in which a sender transmits to everyone in the network.

BER: Bit Error Rate: Percentage of Bits that contain errors relative to the total number of bits transmitted.

Bridge: A device that connects two networks and decides which network the data should go to.

Bridge Mode: Bridge Mode is used when there is one PC connected to the LAN-side Ethernet or USB port. IEEE 802.1D method of transport bridging is used to bridge between the WAN (ADSL) side and the LAN (Ethernet or USB) side, i.e., to store and forward.

CBR: Constant Bit Rate: A constant transfer rate that is ideal for streaming (executing while still downloading) data, such as audio or video files.

Cell: A unit of transmission in ATM, consisting of a fixed-size frame containing a 5-octet header and a 48-octet payload.

CHAP: Challenge Handshake Authentication Protocol: Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

CLP: Cell Loss Priority: ATM cells have two levels of priority, CLP0 and CLP1. CLP0 is of higher priority, and in times of high traffic congestion, CLP1 error cells may be discarded to preserve the Cell Loss Ratio of the CLP0 cells.

CO: Central Office: In a local loop, a Central Office is where home and office phone lines come together and go through switching equipment to connect them to other Central Offices. The distance from the Central Office determines whether or not an ADSL signal can be supported in a given line.

CPE: Customer Premises Equipment. This specifies equipment on the customer, or LAN, side.

CRC: Cyclic Redundancy Checking: A method for checking errors in a data transmission between two computers. CRC applies a polynomial function (16 or 32-bit) to a block of data. The result of that polynomial is appended to the data transmission. Upon receipt, the destination computer applies the same polynomial to the block of data. If the host and destination computer share the same result, the transmission was successful. Otherwise, the sender is notified to re-send the data block.

DHCP: Dynamic Host Configuration Protocol: A communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP). DHCP can lease and IP address or provide a permanent static address to those computers who need it (servers, etc.).

DMZ: Demilitarized Zone: A computer Host or network that acts as a neutral zone between a private network and a public network. A DMZ prevents users outside of the private network from getting direct access to a server or any computer within the private network. The outside user sends requests to the DMZ, and the DMZ initiates sessions in the public network based on these requests. A DMZ cannot initiate a session in the private network, it can only forward packets to the private network as they are requested.

DNS: Domain Name System: A method to locate and translate Domain Names into Internet Protocol (IP) addresses, where a Domain Name is a simple and meaningful name for an Internet address.

DSL: Digital Subscriber Line: A technology that provides broadband connections over standard phone lines.

DSLAM: Digital Subscriber Line Access Multiplexer: Using multiplexing techniques, a DSLAM receives signals from customer DSL lines and places the signals on a high-speed backbone line. DSLAMs are typically located at a telephone company's CO (Central Office).

Encapsulation: The inclusion of one data structure within another. For example, packets can be encapsulated in an ATM frame during transfer.

FEC: Forward Error Correction: An error correction technique in which a data packet is processed through an algorithm that adds extra error correcting bits to the packet. If the transmitted message is received in error, these bits are used to correct the errored bits without retransmission.

Firewall: A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

Fragmentation: Breaking a packet up into smaller packets that is caused either by the transmission medium being unable to support the original size of the packet or the receiving computer not being able to receive a packet of that size. Fragmentation occurs when the sender's MTU is larger than the receiver's MRU.

FTP: File Transfer Protocol. A standardized internet protocol which is the simplest way to transfer files from one computer to another over the internet. FTP uses the Internet's TCP/IP protocols to function.

Full Duplex: Data transmission can be transmitted and received on the same signal medium and at the same time. Full Duplex lines are bidirectional.

G.dmt: Formally G.992.1, G.dmt is a form of ADSL that uses Discrete MultiTone (DMT) technology. G.dmt incorporates a splitter in its design.

G.lite: Formally G.992.2, G.lite is a standard way to install ADSL service. G.lite enables connections speeds up to 1.5 Mbps downstream and 128 kbps upstream. G.lite does not need a splitter at the user end because splitting is preformed at the remote end (telephone company).

Gateway: A point on the network which is an entrance to another network. For example, a router is a gateway that connects a LAN to a WAN.

Half Duplex: Data transmission can be transmitted and received on the same signal medium, but not simultaneously. Half Duplex lines are bi-directional.

HEC: Headed Error Control: ATM error checking by using a CRC algorithm on the fifth octet in the ATM cell header to generate a check character. Using HEC, either a single bit error in the header can be corrected or multiple bit errors in the header can be detected.

HNP: Home Network Processor

Host: In context of Internet Protocol, a host computer is one that has full two way access to other computers on the Internet.

IAD: Integrated Access Device: A device that multiplexes and demultiplexes communications in the CPE onto and out of a single telephone line for transmission to the CO.

IP: Internet Protocol: The method by which information is sent from one computer to another through the Internet. Each of these host computers have a unique IP address which distinguishes it from all the other computers on the internet. Each packet of data sent includes the sender's IP address and the receiver's IP address.

LAN: Local Area Network: A group of computers, typically covering a small geographic area, that share devices such as printers, hard disk drives, scanners, and optical drives. Computers in a LAN typically share an internet connection through some sort of router that connects the computers to a WAN.

LLC: Logical Link Control: Provides an interface point to the MAC sublayer. LLC Encapsulation is needed when several protocols are carried over the same Virtual Circuit.

MAC Address: Media Access Control Address: A unique hardware number on a computer or device that identifies it and relates it to the IP address of that device.

MC: Multicast: Communication involving a single sender and multiple specific receivers in a network.

MRU: Maximum Receive Unit: MRU: Maximum Receive Unit (MRU) is the largest size packet that can be received by the modem. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MSS: Maximum Segment Size: The largest size of data that TCP will send in a single, unfragmented IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their Maximum Segment Size during the TCP connection handshake.

MTU: Maximum Transmission Unit: The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).

NAPT: Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

NAT: Network Address Translation: The translation of an IP address of one network to a different IP address known by another network. This gives an outside (WAN) network the ability to distinguish a device on the inside (LAN) network, as the inside network has a private set of IP address assigned by the DHCP server not known to the outside network.

PAP: Password Authentication Protocol: An authentication protocol in which authorization is done through a user name and password.

PDU: Protocol Data Unit: A frame of data transmitted through the data link layer 2.

Ping: Packet Internet Groper: A utility used to determine whether a particular device is online or connected to a network by sending test packets and waiting for a response.

PPP: Point-to-Point Protocol: A method of transporting and encapsulating IP packets between the user PC and the ISP. PPP is full duplex protocol that is transmitted through a serial interface.

Proxy: A device that closes a straight connection from an outside network (WAN) to an inside network (LAN). All transmissions must go through the proxy to get into or out of the LAN. This makes the internal addresses of the devices in the LAN private.

PVC: Permanent Virtual Circuit: A software defined logical connection in a network; A Virtual Circuit that is permanently available to the user.

RIP: Routing Information Protocol: A management protocol that ensures that all hosts in a particular network share the same information about routing paths. In a RIP, a host computer will send its entire routing table to another host computer every X seconds, where X is the supply interval. The receiving host computer will in turn repeat the same process by sending the same information to another host computer. The process is repeated until all host computers in a given network share the same routing knowledge.

RIPv1: RIP Version 1: One of the first dynamic routing protocols introduced used in the internet, RIPv1 was developed to distribute network reach ability information for what is now considered simple topologies.

RIPv2: RIP Version 2: Shares the same basic concepts and algorithms as RIPv1 with added features such as subnet masks, authentication, external route tags, next hop addresses, and multicasting in addition to broadcasting.

Router Mode: Router Mode is used when there is more than one PC connected to the LAN-side Ethernet and/or USB port. This enables the ADSL WAN access to be shared with multiple nodes on the LAN. Network Address Translation (NAT) is supported so that one WAN-side IP address can be shared among multiple LAN-side devices. DHCP is used to serve each LAN-side device and IP address.

SNAP: SubNetwork Attachment Point.

SNMP: Simple Network Management Protocol: Used to govern network management and monitor devices on the network. SNMP is formally described in RFC 1157.

SNR: Signal-to-Noise Ratio: Measured in decibels, SNR is a calculated ratio of signal strength to background noise. The higher this ratio, the better the signal quality.

Subnet Mask: Short for SubNetwork Mask, subnet mask is a technique used by the IP protocol to filter messages into a particular network segment, called a subnet. The subnet mask consists of a binary pattern that is stored in the client computer, server, or router. This pattern is compared with the incoming IP address to determine whether to accept or reject the packet.

TCP: Transfer Control Protocol: Works together with Internet Protocol for sending data between computers over the Internet. TCP keeps track of the packets, making sure that they are routed efficiently.

TFTP: Trivial File Transfer Protocol: A simple version of FTP protocol that has no password authentication or directory structure capability.

Trellis Code: An advanced method of FEC (Forward Error Correction). When enabled, it makes for better error checking at the cost of slower packet transmission. Setting Trellis Code to Disabled will cause increased packet transmission with decreased error correction.

TTL: Time To Live: A value in an IP packet that indicates whether or not the packet has been propagating through the network too long and should be discarded.

UBR: Unspecified Bit Rate: A transfer mode that is usually used in file transfers, email, etc. UBR can vary depending on the data type.

USB: Universal Serial Bus: A standard interface between a computer and a peripheral (printer, external drives, digital cameras, scanners, network interface devices, modems, etc.) that allows a transfer rate of 12Mbps.

UDP: User Datagram Protocol: A protocol that is used instead of TCP when reliable delivery is not required. Unlike TCP, UDP does not require an acknowledgement (handshake) from the receiving end. UDP sends packets in one-way transmissions.

VBR-nrt: Variable Bit Rate – non real time: With VBR-nrt, cell transfer is variable upon certain criteria.

VC: Virtual Circuit: A virtual circuit is a circuit in a network that appears to be a physically discrete path, but is actually a managed collection of circuit resources that allocates specific circuits as needed to satisfy traffic requirements.

VCI: Virtual Channel Identifier: A virtual channel identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel.

VC-Mux: Virtual Circuit based Multiplexing: In VC Based Multiplexing, the interconnect protocol of the carried network is identified implicitly by the VC (Virtual Circuit) connecting the two ATM stations (each protocol must be carried over a separate VC).

VPI: Virtual Path Identifier: Virtual path for cell routing indicated by an eight bit field in the ATM cell header.

WAN: Wide Area Network: A WAN covers a large geographical area. A WAN is consisted of LANs and the Internet is consisted of WANs.

WPA: Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.